S. Hrg. 112–524

SECURING AMERICA'S FUTURE: THE CYBERSECURITY ACT OF 2012

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

FEBRUARY 16, 2012

Available via the World Wide Web: http://www.fdsys.gov

Printed for the use of the
Committee on Homeland Security and Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

73–673 PDF WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan	SUSAN M. COLLINS, Maine
DANIEL K. AKAKA, Hawaii	TOM COBURN, Oklahoma
THOMAS R. CARPER, Delaware	SCOTT P. BROWN, Massachusetts
MARK L. PRYOR, Arkansas	JOHN MCCAIN, Arizona
MARY L. LANDRIEU, Louisiana	RON JOHNSON, Wisconsin
CLAIRE MCCASKILL, Missouri	ROB PORTMAN, Ohio
JON TESTER, Montana	RAND PAUL, Kentucky
MARK BEGICH, Alaska	JERRY MORAN, Kansas

MICHAEL L. ALEXANDER, *Staff Director*
MARY BETH SCHULTZ, *Associate Staff Director and Chief Counsel for Homeland Security Preparedness and Response*
JEFFREY E. GREENE, *Senior Counsel*
JEFFREY D. RATNER, *Counsel*
MATTHEW R. GROTE, *Professional Staff Member*
NICHOLAS A. ROSSI, *Minority Staff Director*
BRENDAN P. SHIELDS, *Minority Director of Homeland Security Policy*
DENISE F. ZHENG, *Minority Professional Member*
TRINA DRIESSNACK TYRER, *Chief Clerk*
PATRICIA R. HOGAN, *Publications Clerk*
LAURA W. KILBRIDE, *Hearing Clerk*

CONTENTS

WITNESSES

THURSDAY, FEBRUARY 16, 2012

ALPHABETICAL LIST OF WITNESSES

Page

APPENDIX

SECURING AMERICA'S FUTURE: THE CYBERSECURITY ACT OF 2012

THURSDAY, FEBRUARY 16, 2012

U.S. SENATE,
COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 2:32 p.m., in room SD–342, Dirksen Senate Office Building, Hon. Joseph I. Lieberman, Chairman of the Committee, presiding.

Present: Senators Lieberman, Levin, Akaka, Carper, Pryor, Landrieu, Collins, Brown, McCain, Johnson, and Moran.

OPENING STATEMENT OF CHAIRMAN LIEBERMAN

Chairman LIEBERMAN. The hearing will come to order. Senator Collins is on her way. I just saw Senator McCain and Governor Janet Napolitano together, and it seems to me, with the two of you here, I cannot hesitate to offer my congratulations on the centennial celebration of the great State of Arizona. Hear, hear.

Senator MCCAIN. I was there at the time. [Laughter.]

Chairman LIEBERMAN. You look very well for your age.

This is, in fact, the 10th hearing our Committee has held on cybersecurity, and I hope it is the last before the comprehensive cybersecurity bill before us today is enacted into law.

The fact is that time is not on our side.

To me it feels like September 10, 2001, and the question is whether we will act to prevent a cyber 9/11 before it happens instead of reacting after it happens.

The reason for this legislation is based on fact. Every day, rival nations, terrorist groups, criminal syndicates, and individual hackers probe the weaknesses in our most critical computer networks, seeking to steal government and industrial secrets or to plant cyber agents in the cyber systems that control our most critical infrastructure and would enable an enemy, for example, to seize control of a city's electric grid, water supply system, our Nation's financial system, or mass transit networks with the touch of a key from a world away.

The current ongoing and growing cyber threat not only threatens our security here at home, but it is right now having a very damaging impact on our economic prosperity because extremely valuable intellectual property is being stolen regularly through cyber exploitation by individuals, groups, and countries abroad and is then being replicated without the initial cost of research done by

American companies, meaning that jobs are being created abroad that would otherwise be created here.

So when we talk about cybersecurity, there is a natural way in which people focus on the very real danger that an enemy will attack us through cyberspace, but as we think about how to grow our economy again and create jobs again, I have come to the conclusion this is actually one of the most important things we can do to protect the treasures of America's intellectual innovation from being stolen by competitors abroad.

Last year, a very distinguished group of security experts, led by former Department of Homeland Security (DHS) Secretary Michael Chertoff and former Defense Secretary William Perry, going across both parties, issued a stark warning:

"The constant assault of cyber assaults has inflicted severe damage to our national and economic security, as well as to the property of individual citizens. The threat is only going to get worse. Inaction is not an acceptable action." I agree.

The bill before us today is the product of hard work across both party lines and Committee jurisdictional lines. I particularly want to thank my colleagues Senator Collins and Commerce Chairman Jay Rockefeller and Intelligence Committee Chairman Dianne Feinstein for all their hard and cooperative work in getting us to this point. We are going to be privileged to hear from all three of them shortly.

I also want to thank Senator Carper, who is not here yet, for his significant leadership contributions to this effort.

And I want to thank the witnesses who are here. We have chosen the witnesses deliberately because they hold differing points of view on the problem and on the legislation we have crafted and the challenges we face, and we look forward to their testimony.

So the Cybersecurity Act of 2012 does several important things to beef up our defenses in the new battleground of cyberspace.

First, it ensures that the cyber systems that control our most critical, privately owned and operated infrastructure are secure, and that is the key here. Privately owned and operated cyber infrastructure can well be—probably someday will be—the target of an enemy attack. Today it is the target of economic exploitation, and we have to work together with the private sector to better secure those systems, both for their own defense and for our national defense.

In this bill, the systems that will be asked to meet standards are defined as those that, if brought down or commandeered, would lead to mass casualties, evacuations of major population centers, the collapse of financial markets, or significant degradation of our national security. So this is a tight and high standard. After identifying the systems that meet those standards, the Secretary of the Department of Homeland Security under the legislation would then work with the private sector operators of the systems to develop cybersecurity performance requirements.

Owners of the privately operated cyber systems covered would have the flexibility to meet the performance requirements with whatever hardware or software they choose, so long as it achieves the required level of security. The Department of Homeland Security will not be picking technological winners or losers, and in my

opinion, there is nothing in the bill that would stifle innovation. In fact, a letter from Cisco Systems and Oracle, two of our most prominent information technology (IT) companies, concludes that this legislation, "includes a number of tools that will enhance the Nation's cybersecurity without interfering with the innovation and development processes of the American IT industry."

If a company can show under our legislation to the Department of Homeland Security that it already has high cybersecurity standards met, then it will be exempt from further requirements under this law. Failure to meet the standards will result in civil penalties that will be proposed by the Department during a standard rulemaking and comment process.

The bill also creates a streamlined and efficient cyber organization within DHS that will work with existing Federal regulators and the private sector to ensure that no rules or regulations are put in place that either duplicate or are in conflict with existing requirements.

The bill, importantly, also establishes mechanisms for information sharing between the private sector and the Federal Government and among the private sector operators themselves. This is important because computer security experts need to be able to compare notes in order to protect us from this threat. But the bill also creates security measures and oversight to protect privacy and preserve civil liberties. In fact, the American Civil Liberties Union (ACLU) has reviewed our bill and says that it offers the greatest privacy protections of any cybersecurity legislation that has yet been proposed.

I am going to skip over some of the other things the bill does and just go to mention that the process by which we reached this legislative proposal was very inclusive. We not only worked across Committee lines, but reached out to people in business, academics, civil liberties and privacy and security experts for advice on many of the difficult issues that any meaningful piece of cybersecurity legislation would need to address. I can tell you that literally hundreds of changes have been made to this bill as a result of their input, and we think finally we have struck the right balance.

I do want to describe briefly or mention some things that are not in this bill. First and foremost, this bill does not contain a so-called kill switch that would allow the President to seize or control part of or all of the Internet in a national crisis. It is not there.

Senator COLLINS. It never was.

Chairman LIEBERMAN. It never was. Thank you, Senator Collins. But we put an exclamation point by dropping a section, frankly, that people thought included a kill switch. It just was not worth it because of the urgent need for this bill.

There is also nothing in this bill that touches on the balance between intellectual property and free speech that so aroused public opinion over the proposed Stop Online Privacy Act (SOPA) and the Protect IP Act (PIPA) and has left many Members of Congress with scars or at least a kind of post-traumatic stress syndrome since that happened.

So, in fact, this is not the ultimate verification of my assertion that there is nothing here anywhere like what concerned people in SOPA or PIPA, but I note with gratitude that one of our witnesses,

Stewart Baker, was a leading opponent of SOPA but is testifying today in favor of our bill.

After the Cybersecurity Act of 2012 becomes law, the average Internet user will go about using the Internet just as they do today. But hopefully as a result of the law and outreach pursuant to it, they will be far better equipped to protect their own privacy and resources from cyber attack.

The bottom line, a lot of people have worked very hard to come so far and in a very bipartisan way to face a real and present danger to our country that we simply cannot allow this moment to slip away from us. I feel very strongly that we need to act now to defend America's cyberspace as a matter of national and economic security.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you, Mr. Chairman.

Mr. Chairman, let me first applaud you for your leadership in this very important issue, as well as the leadership of our two lead-off witnesses, Senator Rockefeller and Senator Feinstein, who contributed so much to this issue and this bill. And I personally thank you for holding this important hearing today.

After the 9/11 attacks, we learned of many early warnings that went unheeded, including a Federal Bureau of Investigation (FBI) agent, who warned that one day people would die because of the "wall" that kept law enforcement and intelligence agencies apart. When a major cyber attack occurs, the ignored warnings will be even more glaring because our Nation's vulnerability has already been demonstrated by the daily attempts by nation states, terrorists groups, cyber criminals, and hackers to penetrate our systems.

The warnings of our vulnerability to a major cyber attack come from all directions and countless experts, and they are underscored by the intrusions that have already occurred. Earlier this month, the FBI Director warned that the cyber threat will soon equal or surpass the threat from terrorism. He argued that we should be addressing the cyber threat with the same intensity that we have applied to the terrorist threat.

Director of National Intelligence (DNI) James Clapper made the point even more strongly, describing the cyber threat as a "profound threat to this country, to its future, its economy, its very well-being."

In November, the Director of the Defense Advanced Research Projects Agency (DARPA) warned that malicious cyber attacks threaten a growing number of the systems with which we interact every day—the electric grid, water treatment plants, and key financial systems.

Similarly, General Keith Alexander, the Commander of U.S. Cyber Command and the Director of the National Security Agency (NSA), has warned that our cyber vulnerabilities are extraordinary and characterized by "a disturbing trend, from exploitation to disruption to destruction."

These statements are just the latest in a chorus of warnings from current and former officials, and the threat, as the Chairman has pointed out, is not just to our national security but also to our eco-

nomic well-being. A Norton study last year calculated the cost of global cyber crime at $114 billion annually. When combined with the value of time victims lost due to cyber crime, this figure grows to $388 billion. Norton described this as "significantly more" than the global black market in marijuana, cocaine, and heroin combined.

In an op-ed last month entitled, "China's Cyber Thievery Is National Policy—And Must Be Challenged," former DNI Mitch McConnell, former Homeland Security Secretary Michael Chertoff, and former Deputy Secretary of Defense William Lynn noted the ability of cyber terrorists to "cripple" our critical infrastructure. They sounded an even more urgent alarm about the threat of economic cyber espionage.

Citing an October 2011 report by the Office of the National Counterintelligence Executive, these experts warned of the catastrophic impact that cyber espionage—particularly that pursued by China—could have on our economy and competitiveness. They estimated that the cost "easily means billions of dollars and millions of jobs."

This threat is all the more menacing because it is being pursued by a global competitor seeking to steal the research and development of American firms to undermine our economic leadership.

The evidence of our cybersecurity vulnerability is overwhelming. It compels us to act now. Some Members have called for yet more studies, even more hearings, and additional markups. In other words, more delay. The fact is, since 2005, our Committee alone has held 10 hearings on the cyber threat, including today's hearing. I know that the Commerce and the Intelligence Committees have held many more. In 2011, Chairman Lieberman, Senator Carper, and I introduced our cybersecurity bill, which was reported out by this Committee later that same year. Since last year, we have been working with Chairman Rockefeller to merge our bill with legislation that he championed, which was reported by the Commerce Committee. Senator Feinstein has done ground-breaking work on information sharing, which she has been kind enough to share with this Committee, as well.

After incorporating changes based on the feedback from the private sector, our colleagues, and the Administration, we have produced a refined version, which is the subject of today's hearing. And it is significant that three Senate chairmen with jurisdiction over cybersecurity have come together on these issues. And each day that we fail to act, the threat increases to our national and economic security.

Now, other colleagues of ours have urged us to focus narrowly on the Federal Information Security Management Act (FISMA), as well as on Federal research and development (R&D) and improved information sharing. We do need to address these issues, and our bill does just that.

However, with 85 percent of our Nation's critical infrastructure owned by the private sector, the government also has a critical role to play in ensuring that the most vital parts of that infrastructure—those whose disruption could result in truly catastrophic consequences—meet reasonable, risk-based performance standards.

In an editorial this week, the *Washington Post* concurred, writing that our "critical systems have remained unprotected."

Some of our colleagues are skeptical about the need for any new regulations. I have opposed efforts to expand regulations that would burden our economy. But regulations that are necessary for our national security and that promote—rather than hinder—our economic prosperity strengthen our country. They are in an entirely different category.

The fact is the risk-based performance requirements in our bill are targeted carefully. They apply only to specific systems and assets, not entire companies, which if damaged could result reasonably in mass casualties, mass evacuations, catastrophic economic damages, or a severe degradation of our national security. In fact, some of the witnesses think that we have gone too far in that direction.

Senator Lieberman has described much of what the bill contains, so I will not repeat that in the interest of time. Let me just say that this bill is urgent. We cannot wait to act. We cannot wait until our country has a catastrophic cyber attack. And it would be irresponsible of Congress not to pass legislation due to turf battles or due to claims by some businesses that we are somehow harming our economy. In fact, what we are doing is protecting our economy and our way of life.

Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thank you, Senator Collins, for that very strong statement. I agree with you. I would just correct one part. You said how pleased you were that three committee chairs with jurisdiction have come together on the bill. Since I consider you the Co-Chairman of this Committee, I would say it was four.

Senator COLLINS. Thank you.

Chairman LIEBERMAN. And I appreciate very much your contribution to this effort.

We are really grateful to have Senator Rockefeller and Senator Feinstein here. Again, I cannot thank you enough for the work that we have done together. I think it is a very powerful statement that we agreed on a consensus bill, and I hope it enables us to move it through the Senate.

I know the Majority Leader is really concerned about the threat and is committed to giving this bill time on the floor as soon as possible.

Senator Rockefeller, we welcome your testimony now.

TESTIMONY OF HON. JOHN D. ROCKEFELLER IV,[1] A U.S. SENATOR FROM THE STATE OF WEST VIRGINIA

Senator ROCKEFELLER. Thank you, Chairman Lieberman and Senator Collins. And you are quite right about that—I think Senator Harry Reid wants this on the floor as soon as possible. And, frankly, the thing that scares me more than anything is the fact that we have had so many hearings, and yet that was necessary to get to the agreements that we have all come to. And they are solid now, they are rock solid. But we still have to find the floor time for it. This is not going to be an easy time to do that, so the

[1] The prepared statement of Senator Rockefeller appears in the Appendix on page 63.

pressure on this Congress, on both the House and the Senate, to come through on this in the face of all of this danger, this is huge, and not yet guaranteed.

I think our government needs a lead civilian agency to coordinate our civilian cybersecurity efforts, and that agency should, of course, be the Department of Homeland Security under the superb leadership of Secretary Napolitano.

I want to emphasize that our bill represents the expertise and hard work, as both of you have said, of three Senate committees, and that is as it should be.

We have eagerly sought, as you mentioned, Senator Lieberman—and have received—constructive criticism and input from a whole lot of places. I can remember giving a speech, I think 2 years ago, to a business group, presenting ideas that Olympia Snowe and I had for this, and they were just surprised to hear that somebody was willing to listen to their complaints. And there were a lot of them.

Even when people refused to engage with us—and there have been those, even within the Senate, who refuse to have staff discussion, but that does not mean that we do not take some of their suggestions. We have done that because if they do not want to engage, that is OK. If they have good suggestions, then put them in and make it a stronger bill.

Beyond this bill's principal authors—Senators Lieberman, Collins, Dianne Feinstein and myself—the bill reflects the input, assistance, or requests of Senators on both sides of the aisle, as it should be, which gives me hope for final passage.

Senator Olympia Snowe was my co-author of the bill that the Commerce Committee reported out last year, as you know. Senator Carper was a co-author of the Lieberman-Collins bill. Both have left major imprints on this bill.

Senator Kay Bailey Hutchison and her staff worked with us for a good part of the past 2 years. She is my ranking member and absolutely superb—I call her "Co-Chair," too, incidentally—and we have tried hard to address all of her specific concerns. And I think that we have, in fact, met most of her concerns.

We have sought to engage Senator Saxby Chambliss and before him, Senator Kit Bond, in the same fashion. There was some reluctance at some point to discuss, or have staff discussions. It did not make any difference. We were interested in what they had, and if it was something good in what they had, we put it in the bill. We wanted it in the bill. And then it had to pass future tests as we combined all the efforts.

Senators Jon Kyl and Sheldon Whitehouse contributed an entire title regarding cybersecurity awareness. Senators John Kerry, Dick Lugar, Kirsten Gillibrand, and Orrin Hatch did the same on the title regarding diplomacy.

Because of Senator McCain's concerns, we omitted significant language pertaining to the White House Cyber Office.

When colleagues had ongoing questions about a provision that I personally believed to be extremely important, I agreed to drop it from the base bill. This provision that I am talking about would clarify private sector companies' existing requirements regarding what "material risks" pertaining to cyber have to be disclosed to in-

vestors in the Securities and Exchange Commission (SEC) filings because, as you know, at one point out of frustration I went to the SEC and Mary Schapiro agreed to claify that if you are hacked into as a company, it must be disclosed on the Web site of that company at SEC, and that has had a substantial impact, actually.

I believe this provision is absolutely crucial for the market to help solve our cyber vulnerabilities and will fight for it as an amendment on the floor. And that is as it should be. That is the way the system works. But in the interest of providing more time to address colleagues' questions, I agreed to take it out of the bill that we introduced this week.

Any suggestion that this exhaustive process has been anything but open and transparent is patently false. This has been a really open process—and lengthy, as has been pointed out.

Why have we worked so tirelessly to include the views of all sides? Why have we tried so hard to get this right?

Because our country and our communities and our citizens are at grave risk. They simply are. I am not sure if they are aware because there are so many things that are reported in a news cycle that it almost diminishes the overall aggregated weight of the danger. So our citizens have to be aware of this. This is not a Republican or Democrat issue. It is a life-or-death issue for the economy and for us as people.

I want to be clear: The cyber threat is very real fact. This is not alarmism. Here is why. It is hard to talk about this sometimes without seeming alarmist, and yet it simply reflects the truth.

Hackers supported by the governments of China and Russia, and also sophisticated criminal syndicates with potential connections to terrorist groups, are now able to crack the codes of our government agencies, including sensitive ones, and the Fortune 500. They can do that, and they do that on a regular basis.

Senator Collins mentioned what Michael Mullen said, and she pointed out that we are being looted of valuable possessions on an unfathomable scale. But that is not the end of the problem.

The reason that this cyber theft is a life-or-death issue is the same as the reason that a burglar in your house is a life-or-death issue. If a criminal has broken into your home, how do you know what he wants to do? Is it take your belongings or is it something more? You do not know. He is in the building, in your home. That is where we are now in terms of our country.

So that is the situation we face. Cyber burglars have broken in. Mike Mullen has said exactly what Senator Collins indicated, that the only other threat on the same level to cyber threat is Russia's stockpile of nuclear weapons.

I remember the first thing after 9/11 we had to pass, sadly, pathetically, was a law saying that the Central Intelligence Agency (CIA) and the FBI could talk to each other. I mean, how pathetic could that be? But that is where we were because of stovepipes and things of that sort. FBI Director Robert Mueller testified to Congress recently that the cyber threat will soon overcome terrorism as his top national security emphasis. So it is all very serious, and you cannot exaggerate it, and it could happen.

So then you think about how people could die if a cyber terrorist attacked our air traffic control system. And I was talking with Sec-

retary Napolitano just before this hearing. Often over big cities it gets very soupy. Pilots do not like to be in soupy weather. They cannot see above, they cannot see below. Pilots do not like it. But they are protected because of the air traffic control system. We are going to put in a more modern one, but the same situation will prevail. Cyber hackers can take that out of a city or a group of cities. They can take out that capacity so that planes are literally flying in the dark, and they will fly into each other and kill a lot of people. And people have to understand that.

If rail switching networks are hacked, causing trains which carry toxic materials, deadly materials through our major cities, to crash, and there can be a massive explosion from that.

So we are on the brink of very serious happenings. We have not reached that, which is one of our problems in getting legislation passed. But we can act now and try and prepare ourselves.

Let me just close by saying that I was on the Intelligence Committee during the time leading up to 2011, and the world was rife with reports of people coming in and going out of our country, dots here and there that appeared to be connected but we were not quite sure. And what about this Moussaoui thing? And what about folks in that house in San Diego? And all of that was up there. What about the closing down of the bin Laden unit or a message that never got to the bin Laden unit? I mean, all of that was there, and we knew all of that, and the national security apparatus was working very hard on that. And they took it seriously, but they did not get deep enough because it was a new phenomenon.

Well, here we are in a very similar situation. It is already with us. It is much more obvious than the lead-up to 2001 was. And so we now have to act. We do not have the luxury of waiting to see and develop. We have to act. At some point the Congress has to assert itself. The Federal Government does have roles where this is not a heavy-handed thing, as Senator Collins has pointed out. It is not. But the Federal Government is involved because it is a matter of national security. And so I just wait to work with everybody and anybody to get this passed through both Houses of the U.S. Congress.

Chairman LIEBERMAN. Thanks very much, Senator Rockefeller. That was great.

Chairman Feinstein, welcome, and thank you again. You contributed immensely, particularly on the information-sharing section of the bill, and you bring all the expertise and intelligence of the Senate Committee on Intelligence.

TESTIMONY OF HON. DIANNE FEINSTEIN,[1] A U.S. SENATOR FROM THE STATE OF CALIFORNIA

Senator FEINSTEIN. Thank you very much. Thank you, Mr. Chairman, Senator Collins, and Senator Landrieu.

I look at this as quite a banner day because finally the Senate is coming together, and we are settling on one bill. This is the bill, and if it needs improving, we will improve it. But we have a focus now, and with a focus we can hopefully move forward.

[1] The prepared statement of Senator Feinstein appears in the Appendix on page 67.

To this Committee and to Senator Rockefeller's committee, I want to thank you for your hard work, for the dozen hearings you have held, and for all the offers for consultation that you have placed out there to us.

Let me speak for a moment on behalf of what I do in the Intelligence Committee. We have examined cyber threats to our national and economic security, and just last month, at the Worldwide Threats Hearing, which was an open hearing, we heard FBI Director Bob Mueller testify that "the cyber threat, which cuts across all programs, will be the number one threat to the country." And already cyber threats are doing great damage to the United States, and the trend is getting worse.

Let me give you just four examples, and what is interesting is many of us know about these when they happen, but they are often classified or kept private because the people that they happen to do not want it released because their clients will think badly of them. And, of course, it is not their fault, but, nonetheless.

I think it is fair to say that the Pentagon's networks are being probed thousands of times daily, and its classified military computer networks suffered a "significant compromise" in 2008, and that is according to former Deputy Defense Secretary William Lynn.

In November 2009, the Department of Justice (DOJ) charged seven defendants from Estonia, Russia, and Moldova with hacking into the Royal Bank of Scotland and stealing $9 million from more than 2,100 ATMs in 280 cities worldwide in 12 hours.

In 2009, Federal officials indicted three men for stealing data from more than 130 million credit cards by hacking into five major companies' computer systems, including 7-Eleven, Heartland Payment Systems, and the Hannaford Brothers supermarket chain.

Finally, an unclassified report by the intelligence community in November 2011 said cyber intrusions against U.S. companies cost untold billions of dollars annually, and that report named China and Russia as aggressive and persistent cyber thieves.

Modern warfare is already employing cyber attacks, as seen in Estonia and the Republic of Georgia. And, unfortunately, it may only be a matter of time before we see cyber attacks that can cause catastrophic loss of life in the United States, whether by terrorists or state adversaries.

Our enemies are constantly on the offensive, and in the cyber domain, it is much harder for us to play defense than it is for them to attack. The hard question is: What do we do about this dangerous and growing cyber threat?

I believe the comprehensive bill that has been introduced—the Cybersecurity Act of 2012—is an essential part of the answer.

Mr. Chairman, I would like to speak briefly on the cybersecurity information-sharing bill that I introduced on Monday and that you have included as Title VII in your legislation.

The goal of this bill is to improve the ability of the private sector and the government to share information on cyber threats that both need to improve their defenses.

However, a combination of existing law, the threat of litigation, and standard business practices has prevented or deterred private sector companies from sharing information about the cyber threats

they face and the losses of information and money they suffer. We need to change that through better information sharing, in a way that companies will use, that protects privacy interests, and that takes advantage of classified information without putting that information at risk. So here is what we have tried to do in Title VII:

One, affirmatively provide private sector companies the authority to monitor and protect the information on their own computer networks.

Two, encourage private companies to share information about cyber threats with each other by providing a good-faith defense against lawsuits for sharing or using that information to protect themselves.

Three, require the Federal Government to designate a single focal point for cybersecurity information sharing. We refer to this as a "Cybersecurity Exchange," to serve as a hub for appropriately distributing and exchanging cyber threat information between the private sector and the government. This is intended to reduce government bureaucracy and make the government a more effective partner in the private sector, but with protections to ensure that private information is not misused. Also, this legislation provides no new authority for government surveillance.

Four, we establish procedures for the government to share classified cybersecurity threat information with private companies that can effectively use and protect that information. This, we believe, is a prudent way to take advantage of the information that the intelligence community acquires, without putting our sources and methods at risk, or turning private cybersecurity over to our intelligence agencies.

I would like to raise just one issue of something that is not yet included in this bill, and that is data breach notification.

This is an issue I have worked on for over 8 years, since California had a huge data breach that we only inadvertently found out about that had literally hundreds of thousands of victims. It is an urgent need. I have a bill called the Data Breach Notification Act. It has been voted out of the Judiciary Committee, and it accomplishes what in my view are the key goals of any data breach notification legislation:

One, notice to individuals, who will be better able to protect themselves from identity theft;

Two, notice to law enforcement, which can connect the dots between breaches and cyber attacks;

And, three—and this is important—preemption of the 47 different State and territorial standards on this issue. This is a real problem. We have 47 different laws on this issue in this country. It makes it very difficult for the private sector. Companies will not be subjected to conflicting regulation if there is one basic standard across the country.

I know that Senators Rockefeller and Pryor have a bill in the Commerce Committee and that Senators Patrick Leahy and Richard Blumenthal have their own bills that also were reported out of the Judiciary Committee.

But the differences in our approaches are not so great that we cannot work them out, and I am very prepared to sit down with Members of this Committee, with Senator Rockefeller, and others

to find a common solution. But Mr. Chairman, I would really implore you to add a data breach preemption across the United States so that there is one standard for notification to an individual of data breach, and communication with law enforcement that goes all across America. Until we have that, we really will not have a sound data breach system.

Let me just thank you. I think we are on our way. I am really so proud of both of you on this Committee for coming together, and I think it is a banner day. So thank you very much.

Chairman LIEBERMAN. Thanks very much, Senator Feinstein. We could not have done it without you. Thanks for your testimony, and I am personally very supportive of your aims with the data breach proposal, and I look forward to working with you and, as you say, the others who have bills to see if we cannot find a way to include that in this proposal when it comes to the floor.

Senator FEINSTEIN. Thank you very much.

Chairman LIEBERMAN. Thank you very much.

And now, Madam Secretary, I hate to break up a conversation between the current Secretary and the first Secretary, but—we almost had the trifecta of the three Secretaries of the Department of Homeland Security here today. Secretary Chertoff wanted to testify, but had a previous commitment, and has, I will say, filed a statement for the record strongly in support of the legislation.[1]

Secretary Napolitano, thanks very much for being here and for all the work you and people in the Department have done to help us come to this point with this bill. We welcome your testimony now.

TESTIMONY OF HON. JANET A. NAPOLITANO,[2] SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Secretary NAPOLITANO. Well, thank you, Chairman Lieberman, Senator Collins, and Members of the Committee. I am pleased to be here today to discuss the issue of cybersecurity and, in particular, the Department's strong support for the Cybersecurity Act of 2012.

I appreciate this Committee's support of the Department's cybersecurity efforts. Your sustained attention to this issue and the leadership you have shown in bringing a bill forward to strengthen and improve our cybersecurity authorities. I also appreciate and want to emphasize the urgency of the situation.

Indeed, the contrast between the urgent need to respond to the threats we face in this area on the one hand and the professed desire for more deliberation and sensitivity to regulatory burdens on the other reminds me, as several of you have suggested, of lessons we learned from the 9/11 attacks. As the 9/11 Commission noted, those attacks resulted, in hindsight, from a failure of imagination because we failed to anticipate the vulnerabilities of our security infrastructure.

There is no failure of imagination when it comes to cybersecurity. We can see the vulnerabilities. We are experiencing the attacks,

[1] The prepared statement of Secretary Chertoff appears in the Appendix on page 108.
[2] The prepared statement of Secretary Napolitano appears in the Appendix on page 71.

and we know that this legislation would materially improve our ability to address the threat.

No country, industry, community, or individual is immune to cyber risks. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services.

Cyber incidents have increased dramatically over the last decade. There have been instances of theft and compromise of sensitive information from both government and private sector networks, and all of this undermines confidence in these systems and the integrity of the data they contain.

Combating evolving cyber threats is a shared responsibility that requires the engagement of our entire society, from government and law enforcement to the private sector and, most importantly, with members of the public. DHS plays a key role in this effort, both in protecting Federal networks and working with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities.

In fiscal year 2011, our U.S. Computer Emergency Readiness Team (US–CERT) teams at DHS received over 106,000 incident reports from Federal agencies, critical infrastructure, and our industry partners. We issued over 5,200 actionable cyber alerts that were used by private sector and government network administrators to protect their systems. We conducted 78 assessments of control system entities and made recommendations to companies about how they can improve their own cybersecurity.

We distributed 1,150 copies of our cyber evaluation tool. We conducted over 40 training sessions on them, all of which makes owners and operators better equipped to protect their networks.

To protect Federal civilian agency networks, we are deploying technology to detect and block intrusions of these networks in collaboration with the Department of Defense. We are providing guidance on what agencies need to do to protect themselves and are measuring implementation of those efforts.

We are also responsible for coordinating the national response to significant cyber incidents and for creating and maintaining a common operational picture for cyberspace across the entire government.

With respect to critical infrastructure, we work with the private sector to help secure the key systems upon which Americans, including the Federal Government, rely, such as the financial sector, the power grid, water systems, and transportation networks.

We pay particular attention to industrial control systems which control processes at power plants and transportation systems alike. Last year, we deployed seven response teams to such critical infrastructure organizations at their request in response to important cyber intrusions.

To combat cyber crime, we leverage the skills and resources of DHS components such as the Secret Service, Immigration and Customs Enforcement (ICE), and Customs and Border Protection (CBP), and we work very closely with the FBI.

DHS serves as the focal point for the government's cybersecurity outreach and public awareness efforts. As we perform this work, we are mindful that one of our missions is to ensure that privacy, confidentiality, and civil liberties are not diminished by our efforts. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset, and we are pleased to see these in the draft bill.

Now, Administration and private sector reports going back decades have laid out cybersecurity strategies and highlighted the need for legal authorities. In addition to other statutes, the Homeland Security Act of 2002 specifically directed DHS to enhance the security of non-Federal networks by providing analysis and warnings, crisis management support, and technical assistance to State and local governments, and the private sector. Policy initiatives have had to supplement the existing statutes. These initiatives strike a common chord. Indeed, this Administration's Cyberspace Policy Review in 2009 echoed in large part a similar review by the Bush Administration, and we have had numerous contributions by private sector groups, including the Center for Strategic and International Studies (CSIS) study led by James Lewis, one of your witnesses today.

Still, DHS executes its portion of the Federal cybersecurity mission under an amalgam of authorities that have failed to keep up with the responsibilities with which we are charged.

To be sure, we have taken significant steps to protect against evolving cyber threats, but we must recognize that the current threat outpaces our existing authorities. Our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated.

We have had many interactions with this Committee and with the Congress to provide our perspective on cybersecurity. Indeed, in the last 2 years, Department representatives have testified in 16 Committee hearings and provided 161 staff briefings. We have had much bipartisan agreement. In particular, many would agree with the House Republican Cyber Task Force, which stated that, "Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity."

The recently introduced legislation contains great commonality with the Administration's ideas and proposals, including two crucial concepts that are central to our efforts: First, addressing the urgent need to bring core critical infrastructure to a baseline level of security; and, second, fostering information sharing, which is absolutely key to our security efforts.

All sides agree that Federal and private networks must be better protected and that information should be shared more easily, yet still more securely. And both our proposal and the Senate legislation would provide DHS with clear statutory authority commensurate with our cybersecurity responsibilities and remove legal barriers to the sharing of information.

S. 2105 would expedite the adoption of the best cybersecurity solutions by the owners and operators of critical infrastructure and give businesses, States, and local governments the immunity they

need to share information about cyber threats or incidents. There is broad support as well for increasing the penalties for cyber crimes and for creating a uniform data breach reporting regime to protect consumers. This proposal would make it easier to prosecute cyber criminals and establish national standards, requiring businesses and core infrastructure that have suffered an intrusion to notify those of us who have the responsibility for mitigating and helping them mitigating it.

I hope that the current legislative debate maintains the bipartisan tenor it has benefited from so far and builds from the consensus that spans two Administrations and the Committee's efforts of the last several years.

Let me close by saying that now is not the time for half measures. As the Administration has stressed repeatedly, addressing only a portion of the needs of our cybersecurity professionals will continue to expose our country to serious risk.

For example, only providing incentives for the private sector to share more information will not in and of itself adequately address critical infrastructure vulnerabilities. And let us not forget that innumerable small businesses rely on this critical infrastructure for their own survival.

As the President noted in the State of the Union address, "The American people expect us to secure the country from the growing danger of cyber threats and to ensure the Nation's critical infrastructure is protected." And as the Secretary of Homeland Security, I strongly support the proposed legislation because it addresses the need, the urgency, and the methodology for protecting our Nation's critical infrastructure. I can think of no more pressing legislative proposal in the current environment.

I want to thank you again for the important work you have done, and I look forward to answering the Committee's questions.

Chairman LIEBERMAN. Thanks very much, Madam Secretary.

We will do 6-minute rounds of questions because we have a large number on the following panel, and I know some people have to leave.

Madam Secretary, let me get right to one of the issues that has been somewhat in contention, which is that there are some people who have said that the expanded authority here, particularly that related to cyber infrastructure owned and operated by the private sector, would better be handled by the Department of Defense (DOD) or the intelligence community. In other words, they should take the lead in protecting Federal civilian networks.

I wonder if you would respond as to why you think the Department of Homeland Security, as obviously we do, is better prepared to take on this critical responsibility.

Secretary NAPOLITANO. Well, several points. First, the Department of Homeland Security, as I stated, already is exercising authorities in the civilian area, working with the private sector, working with Federal civilian agencies. So that is a space we are already filling and continue to grow our capacity to fill.

Second, military and civilian authorities and missions are different, and there are significant differences, for example, in the privacy protections that we employ within the exercise of civil jurisdiction.

And then, finally, I would note that both DOD and DHS use the technological expertise of the NSA. We are not proposing and have never proposed that two NSAs be created; rather, that there be two different lines of authority that emanate using the NSA, one, of course, for civilian, and one for military.

Chairman LIEBERMAN. That is a very important factor. I want to come back to that in a minute. But one of the opinions expressed to the Committee as we faced the challenge and decided which part of our government should be responsible for responding was that there would probably be very deep and widespread concern among the public if we, for instance, asked the National Security Agency or the Department of Defense to be directly in charge of working with the privately owned and operated cyber infrastructure. Particularly for NSA, there would be a concern about privacy and civil liberties concerns. Does that make sense to you?

Secretary NAPOLITANO. I have heard the same concerns. They do make sense. And, indeed, when Secretary Robert Gates and I, by a Memorandum of Understanding, figured out the division of responsibilities and how we were each going to use the NSA, one of the things we were careful to elevate was a discussion of the protections of privacy and civil liberties, and make sure that, to the extent we have people over at the NSA, they are accompanied by people from our Office of Privacy, our Office of General Counsel, to make sure those protections are abided by.

Chairman LIEBERMAN. Right. I am glad you mentioned that Memorandum of Understanding between the Department of Homeland Security and DOD because I want to make this point—incidentally, Senator McCain and I codified that in law, that Memorandum of Understanding, in the National Defense Authorization Act that was passed at the end of last year. But that memorandum, if I can put it this way, does not preempt the need for this legislation. In other words, that memorandum does not allocate responsibility with regard to working with the private sector, having the authority to require the private sector to take steps to defend themselves and our country from cyber attack. Is that right?

Secretary NAPOLITANO. That is right, Mr. Chairman. It is a memorandum that describes the division of how we would each use the resources of the NSA, but it does not deal with the protection of core critical infrastructure the way the bill does. It does not deal with the private sector at all the way the bill does. It does not deal with information exchange the way the bill does. So it really was designed to make sure that at least with respect to how we each use the NSA, we had some meeting of the minds.

Chairman LIEBERMAN. So there is nothing in your opinion inconsistent between the Memorandum of Understanding between DHS and NSA and the Cybersecurity Act of 2012?

Secretary NAPOLITANO. Oh, not at all.

Chairman LIEBERMAN. I am pleased to note for the record that in testimony earlier this week, Secretary of Defense Leon Panetta and the Chairman of the Joint Chiefs of Staff General Martin Dempsey both endorsed this legislation, and then this morning, before the Armed Services Committee, the Director of National Intelligence Clapper and General Ronald Burgess, the head of the Defense Intelligence Agency, also endorsed the legislation. Both of

those expressions of support were unexpected by Senator Collins and me and, therefore, all the more appreciated.

DHS's Industrial Control Systems Cyber Emergency Response Team (ICS–CERT) has played a critical role in providing support to the owners and operators of critical infrastructure. Can you describe some of their capabilities and the work that they have done to assist private entities?

Secretary NAPOLITANO. Well, what they have done is to help isolate and identify—when they have been notified of attacks on industrial control systems, to help identify the source of the attack, the methodology with which it was conducted, to work with the infiltrated entity to prepare a patch, and then to make appropriate disclosures or sharing of information to other control systems that could be subject to a similar tack, either in that particular industry or in other industries.

Chairman LIEBERMAN. So on a voluntary basis, if I can put it this way, DHS has developed the capability and relationships at working with the private sector that will be strengthened by this legislation?

Secretary NAPOLITANO. Yes. Since the passage of the National Information Infrastructure Protection Act (NIIPA) in 2006, we have been working with critical infrastructure through their Sector Coordinating Councils. There are a lot of names, but what it basically means is we have a process in place for dealing with the private sector and for exchanging some information on a voluntary basis. But that does not mean we get all of the necessary information we get from core critical infrastructure. That is one of the problems the bill address.

Chairman LIEBERMAN. Thanks very much. My time is up. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Madam Secretary, to follow up on a question that the Chairman asked you, it is my understanding that DHS has unique expertise in the area of industrial control systems that is not replicated at any other government agency. Is that correct?

Secretary NAPOLITANO. Yes.

Senator COLLINS. And that is important because industrial control systems are a key part of critical infrastructure, like the electric grid and water treatment plants. Is that also correct?

Secretary NAPOLITANO. Yes, and when you think about it, if you have the ability to interrupt the control system, you can take down an entire protective network. You can interfere with all of the activities there. And the attacks on control systems are growing more and more sophisticated all of the time.

Senator COLLINS. And could you tell us about work that is being done by DHS with your ICS–CERT Team and a National Lab with respect to the U.S. electric grid?

Secretary NAPOLITANO. Yes, we are working in both of those capacities with the National Labs, with the grids, in terms not only of mitigating attacks that have occurred, but also preventive measures that they can employ.

Senator COLLINS. So you are doing training as well and helping the critical infrastructure owners and operators identify vulnerabilities?

Secretary NAPOLITANO. That is correct.

Senator COLLINS. It is my understanding that in January the Administration transferred the Defense Department's Defense Industrial Base (DIB) cyber pilot program from DOD to DHS.

Secretary NAPOLITANO. That is right, the DIB pilot.

Senator COLLINS. The DIB pilot program, as I understand it, shared classified cyber threat indicators with defense contractors in an effort to better defend systems that contained information critical to the Department's programs and operations. I understand that DHS is now the lead for coordinating this program with the private sector and that it is being expanded to other critical infrastructure sectors.

Could you tell the Committee why the Administration decided to transfer this pilot program from DOD to the Department of Homeland Security?

Secretary NAPOLITANO. Well, the DIB pilot really gets to the division of responsibility between military and civilian, and what we are talking about here are private companies that do important defense contracting work, but they are in essence private companies. And so the authorities and the laws that we use are better situated in DHS, which deals in this context as opposed to DOD. So we have been working with DOD from the outset on the design of the DIB pilot, have been working with them on the initial aspects of it, and now as the decision was made to extend it and to grow it, the decision was also made that it is more appropriately located within the DHS.

Senator COLLINS. The bill provides the authority to DHS to set risk-based performance standards for critical infrastructure. Do you believe that we can achieve great progress in improving our cybersecurity in this country absent that authority?

Secretary NAPOLITANO. I think it makes it tougher. We have, as I said in my testimony, the basic authority under the Homeland Security Act. We have authorities by various Presidential directives. But nowhere do we have explicit authority to establish on a risk-based level, on a risk-based basis, the protection necessary for critical infrastructure.

Senator COLLINS. Finally, I think that a lot of people are unfamiliar with a lot of the work that the Department has already done in the area of cybersecurity, including the fact that there is a 24-hour, 7-day-a-week National Cybersecurity and Communications Integration Center (NCCIC).

Secretary NAPOLITANO. The NCCIC, yes.

Senator COLLINS. Could you explain to the Committee and those watching this hearing how this center operates and what it does with respect to the private sector?

Secretary NAPOLITANO. You know, the NCCIC is really an integrated, 24/7 watch center for cyber, and it includes on its floor not only DHS employees but representatives from other Federal agencies, from critical infrastructure sectors that coordinate with us through the National Infrastructure Protection Plan (NIPP)—lots of acronyms in the cyber world and the government world. And then, finally, it also has representatives from State and local governments as well because a lot of the information sharing is applicable to them.

Senator COLLINS. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Collins. Senator McCain.

OPENING STATEMENT OF SENATOR MCCAIN

Senator MCCAIN. Mr. Chairman and Senator Collins, thank you for holding this hearing on the long-awaited Cybersecurity Act of 2012. Obviously, I welcome all of our witnesses, including Secretary Napolitano and my old friend Governor Ridge, who will have some different aspects and views on this bill, including in his testimony.

I would like to state from the outset my fondness and respect for the Chairman and Senator Collins, especially when it comes to matters of national security, so the criticisms I may have with the legislation should not be interpreted as criticism of them but, rather on the process by which the bill is being debated and its policy implications.

All of us recognize the importance of cybersecurity in the digital world. Time and again, we have heard from experts about the importance of possessing the ability to effectively prevent and respond to cyber threats. We have listened to accounts of cyber espionage originating in countries like China; organized cyber criminals in Russia; and rogue outfits with a domestic presence like "Anonymous," who unleash cyber attacks on those who dare to politically disagree. Our own Government Accountability Office (GAO) has reported that over the last 5 years, cyber attacks against the United States are up 650 percent. So all of us agree that the threat is real.

It is my opinion that Congress should be able to address this issue with legislation a clear majority of us can support. However, we should begin with a transparent process which allows lawmakers and the American public to let their views be known. Unfortunately, the bill introduced by the Chairman and Senator Collins has already been placed on the calendar by the Majority Leader, without a single markup or any executive business meeting by any committee of relevant jurisdiction. My friends, that is wrong.

To suggest that this bill should move directly to the Senate floor because it has "been around" since 2009 is outrageous. First, the bill was introduced 2 days ago. Second, where do Senate Rules state that a bill's progress in a previous Congress can supplant the necessary work on that bill in the present one?

Additionally, in 2009, we were in the 111th Congress with a different set of Senators. For example, the Minority of this Committee has four Senators on it presently who were not even in the Senate, much less on this Committee, in 2009. How can we seriously call it a product of this Committee without their participation in Committee executive business?

Respectfully, to treat the last Congress as a legislative mulligan by bypassing the Committee process and bringing the legislation directly to the floor is not the appropriate way to begin consideration of an issue as complicated as cybersecurity.

In addition to these valid process concerns, I also have policy issues with the bill.

A few months ago, as Senator Lieberman mentioned, he and I introduced an amendment to the defense authorization bill codifying

an existing cybersecurity Memorandum of Agreement (MOA) between the Department of Defense and the Department of Homeland Security. The purpose of that amendment was to ensure that this relationship endures and to highlight that the best government-wide cybersecurity approach is one where DHS leverages not duplicates DOD efforts and expertise. This legislation, unfortunately, backtracks on the principles of the MOA by expanding the size, scope, and reach of DHS and neglects to afford the authorities necessary to protect the homeland to the only institutions currently capable of doing so, U.S. Cybercommand and the National Security Agency.

At a recent FBI-sponsored symposium at Fordham University, General Alexander, the Commander of U.S. Cybercommand and the Director of the NSA, stated that if a significant cyber attack against this country were to take place, there may not be much that he and his teams at either Cybercommand or NSA can legally do to stop it in advance. According to General Alexander, "in order to stop a cyber attack, you have to see it in real time, and you have to have those authorities. Those are the conditions we have put on the table. Now how and what the Congress chooses, that will be a policy decision."

This legislation does nothing to address this significant concern, and I question why we have yet to have a serious discussion about who is best suited, which agency—who is best suited to protect our country from this threat we all agree is very real and growing.

Additionally, if the legislation before us today were enacted into law, unelected bureaucrats at the DHS could promulgate prescriptive regulations on American businesses—which own roughly 90 percent of critical cyber infrastructure. The regulations that would be created under this new authority would stymie job creation, blur the definition of private property rights, and divert resources from actual cybersecurity to compliance with government mandates. A super-regulator, like DHS under this bill, would impact free market forces which currently allow our brightest minds to develop the most effective network security solutions.

I am also concerned about the cost of this bill to the American taxpayer. The bill before us fails to include any authorizations or attempt to pay for the real costs associated with the creation of the new regulatory leviathan at DHS. This attempt to hide the cost is eclipsed by the reality that the assessment of critical infrastructure, the promulgation of regulations, and their enforcement will take a small army.

Finally, I would like to find out over the next few days what specific factors went into providing regulatory carve-outs for the IT hardware and software manufacturers? My suspicion is that this had more to do with garnering political support and legislative bullying than sound policy considerations. However, I think the fact that such carve-outs are included only lends credence to the notion that we should not be taking the regulatory approach in the first place.

Because of provisions like these and the threat of a hurried process, a total of seven of us—ranking minority members on seven committees—are left with no choice but to introduce an alternative cybersecurity bill in the coming days. The fundamental difference

in our alternative approach is that we aim to enter into a cooperative relationship with the entire private sector through information sharing rather than an adversarial one with prescriptive regulations. Our bill, which will be introduced when we return after the Presidents Day recess, will provide a common-sense path forward to improve our Nation's cybersecurity defenses. We believe that by improving information sharing among the private sector and government, updating our criminal code to reflect the threat cyber criminals pose, reforming the Federal Information Security Management Act, and focusing Federal investments in cybersecurity, our Nation will be better able to defend itself against cyber attacks. After all, we are all partners in this fight, and as we search for solutions, our first goal should be to move forward together.

I also would ask permission to enter in the record a letter signed by Senator Chambliss, the Ranking Member on Intelligence; myself, Ranking Member on Armed Services; Senator Jeff Sessions, Ranking Member on Budget; Senator Michael B. Enzi, Ranking Member on the HELP Committee; Senator Hutchison, Ranking Member on the Commerce Committee; Senator Lisa Murkowski, Ranking Member on the Energy Committee; and Senator Chuck Grassley, Ranking Member on the Judiciary Committee; addressed to Senator Reid and Senator McConnell, which we have asked that with the legislation go through the regular process with the committees of jurisdiction having a say in this process.[1]

So, Mr. Chairman, I thank you, and I yield the remaining balance of my time.

Chairman LIEBERMAN. No balance. [Laughter.]

Senator MCCAIN. Oh, wow, that is the first time that has ever happened.

Chairman LIEBERMAN. No, it is not. [Laughter.]

Look, with the same fondness and respect that you expressed for Senator Collins and me when you started, I cannot conceal the fact that I am disappointed by your statement. This bill is essentially the one that was marked up by the Committee. But that is not the point. The point is that we have reached out not only to everybody who was possibly interested in this bill outside of the Congress, but opened the process to every Member of the Senate who wanted to be involved. We pleaded for involvement. And a lot of people, including yourself, have not come to the table.

The most encouraging part of your statement is that you and those working with you are going to introduce some legislation, and we will be glad to consider it. The Senate should consider it. I think Senator Reid intends to hold an open amendment process on this bill. But you know, as you stated, that this is a critical national security problem, and to respond to it with business about regulation of business, this is national security. As Senator Collins said, there is regulation of business that is bad for business and bad for the American economy. There is regulation such as we have worked very hard to include in this bill that, in fact, is not only not bad for American business and not bad for the American econ-

[1] The letter dated February 14, 2012, submitted by Senator McCain appears in the Appendix on page 61.

omy but will protect American business and American jobs and help to guarantee more American economic growth.

On the question of DOD and the intelligence community, I indicated for the record earlier that they have supported our bill this week. I hear what you said about General Alexander from NSA, but he has at no point, nor has the Department of Defense or the DNI, come before us and offered any suggestions for additions to this bill that would give him more authority. I would welcome those suggestions, if he wishes.

So I had to be honest with you, as you have been honest with us, and express my disappointment and that the only satisfaction I have from your statement, which is that you are going to make a proposal that our colleagues in the Senate consider it. Senator Collins and I and the others working on this bill will consider it. And let us get something done on a clear and present danger to our country this year.

Senator MCCAIN. Well, Mr. Chairman, could I just briefly respond? I speak for seven ranking members of the major committees of jurisdiction. I do not speak just for myself. There is a breakdown somewhere if seven ranking members of the relevant committees are all joining in this opposition to this process and this legislation. So if you choose to neglect those many years of legislative experience and time in the Senate, that is fine. But there are seven of us that are deeply concerned about this process and the legislation, and we do not think it should go directly to the floor.

Chairman LIEBERMAN. I will say for the record that we have reached out to all seven ranking members in various ways to try to engage their involvement in this bill. I would have much rather preferred to submit a bill—and Senator Collins would have, too—that everybody had been involved in discussing. We were very open to trying to find consensus, as we did with other chairs who are here. So nobody is neglecting the expertise. I am saying I am sorry that they have not been engaged before, and I am glad they are going to be engaged now.

Senator Moran.

OPENING STATEMENT OF SENATOR MORAN

Senator MORAN. Mr. Chairman, thank you.

Madam Secretary, this is my first opportunity to visit with you since the announcement about the President's budget, and I want to talk about a topic unrelated at least to cybersecurity, but certainly related to security. And the Chairman just spoke about clear and present danger. One that you and I have had a conversation about over a long period of time is related to our food and animal safety and security in this country. And as you can imagine and can expect the disappointment that I have, others in our congressional delegation have in regard to the President's failure to include dollars related to construction of the National Bio and Agro-Defense Facility (NBAF) to replace the aging Plum Island. You and I have had a number of conversations, and I will stay within my 6 minutes today to talk about this non-germane topic but we will have a greater chance to visit in the Homeland Security Appropriations hearing in which you and I will be together in just a few days.

But I would not want this opportunity to pass without again delivering the message to you and to the folks at the Department of Homeland Security who have throughout this process been our allies, and we consider that we have been your allies in an effort to see that a facility designed to make certain that the food and animal safety of this country is protected.

And you and I had a conversation in March of last year, less than a year ago, that was in a Homeland Security Appropriations Subcommittee, and you told me that NBAF is something that we are very supportive of. Plum Island does not meet the Nation's needs in this area. There was a highly contested, peer-reviewed competition, and we look forward to continued construction. We believe that NBAF needs to be built, and we need to get on with it.

Later, in September of that year, you talked about the future, we need to get prepared for the next generation, and, again, we need to be confronting the things that we face today and the things that we will face 10 years from now. That series has continued with your testimony and others from DHS, the U.S. Department of Agriculture, and I just would like for you to, I hope, reiterate the Department's, your position as Secretary, continued support and believe in the importance of building this facility and to explain to me the idea of a reassessment, which, as I read in press reports, is a reassessment in scope only, not in concerns about safety or concerns about location.

Secretary NAPOLITANO. That is right, Senator, and you are right, the President does not request in the budget an appropriation for the NBAF, in part because last year we requested $150 million. The House ultimately appropriated $75 million, the Senate appropriated zero, we ended up with $50 million, and a lot of extra requirements put on the project, as you just have stated.

What we have done in this year's budget is allocate $10 million that will go to related animal research at Kansas State University. I have talked this over with Governor Sam Brownback, among others. And in light of the Budget Control Act (BCA) and the other changed circumstances that we have to deal with, and in light of the fact that we have not been able to persuade the Congress to really move forward in a substantial way on funding the NBAF, we have recommended that there be a reassessment in terms not of location, not in terms of need, both of which I firmly stand by the position I have stated, but in terms of scoping and what needs to happen so that this project can move forward with the right level of appropriation.

Senator MORAN. Well, Madam Secretary, thank you. I would comment that the solution to lack of funding by Congress is not for the Administration to not request funding. The solution to that problem is continued support and encouragement for Congress to act. As you say, the House appropriated $75 million last year. In a conference committee with the Senate, it was agreed upon to $50 million. You also are requesting reprogramming for additional planning of money within this year's budget. Again, the money that is there needs to be spent as quickly as possible.

I will be asking you by letter shortly to continue the funding of the $40 million that is available, is appropriated, and now as a re-

sult of the report filed this week can be spent to complete the Federal share of the utility portion of this facility.

Based upon what I have heard you say and what I have read that you have said, it is not about location, it is not about the site, and it may be about the scope of what will occur. But the utility pad is still important and will be necessary, regardless of the scope of that project. So we are going to ask you to continue the funding that you already have committed to and are authorized to now spend this $40 million on utilities. And I would add to that point, we have appropriated $200 million Federal dollars. The State of Kansas has put in nearly $150 million. This is a partnership. And we need the Federal Government to continue its partnership. In fact, on the utility portion, we are waiting on the share that you are now authorized to spend to be spent.

I appreciate the answer to my question. I have considered you an ally and continue to consider you an ally. And my plea is let us work together to see that this Congress moves forward on an issue that is important, just as cybersecurity is, to the economic security and future of our Nation.

Mr. Chairman, thank you.

Secretary NAPOLITANO. Senator, I would be happy to work together with you on this.

Senator MORAN. Thank you very much. We need your help.

Chairman LIEBERMAN. Thanks very much, Senator Moran.

For the information of the Members, the order of arrival today now is Senators Landrieu, Pryor, Brown, Carper, Levin, and Johnson. Senator Landrieu is not here, so we will go to Senator Pryor.

OPENING STATEMENT OF SENATOR PRYOR

Senator PRYOR. Thank you, Mr. Chairman. Thank you for this very important meeting. Always good to see you, Madam Secretary.

Let me start, Madam Secretary, with a question about—I think you have already pretty much said that you feel like we need a statute, but I am curious about what specific authority you think your agency or the Federal Government does not have in this area that you need. What specific authority do you feel like you need to accomplish to achieve security in this area?

Secretary NAPOLITANO. Well, I think of the specific authorities that the statute contains, the most important is the ability to bring all of the Nation's critical infrastructure up to a certain base standard of security and to outline the process with which that will occur.

Senator PRYOR. And let me ask you a question on a different topic, I know that in reading some of the news stories, trade publications, etc., the private sector seems to have hesitation about sharing too much information, and understandably so. They may fear that a competitor will get information or it may create liability issues for them. But we do have an effective mechanism for the private sector stakeholders to share their best practices and potential threats and those concerns without raising issues of their own security and liability and even antitrust concerns?

Secretary NAPOLITANO. No. In fact, another major improvement in the bill over the current situation is it clarifies the kind of information sharing that can occur without violating other Federal stat-

utes—antitrust, the Electronic Communications Privacy Act. We have had situations where we have had delay in being able to get information and to respond because the lawyers of a company or an entity had to first assess whether they would be violating other Federal law by alerting the Department of Homeland Security that an intrusion had occurred. And I think as you and I can both appreciate, when the lawyers get it, it can take awhile.

Senator PRYOR. We understand.

Secretary NAPOLITANO. So, again, the new bill would clarify that should not be a problem.

Senator PRYOR. And you are comfortable with how the new bill is structured in that area?

Secretary NAPOLITANO. Yes, I am.

Senator PRYOR. And let me ask about lessons learned. DHS has recently discussed—and it has been discussed about DHS—that some of the work being done under the Chemical Facility Anti-Terrorism Standards (CFATS) program has not been done as quickly or as thoroughly as maybe it should have been. And as you know, this bill provides a requirement that DHS would do similar type assessments. Are there lessons learned in the CFATS experience that might indicate that we can put the problem behind us and we can comply with what this law would ask you to do?

Secretary NAPOLITANO. Yes, Senator. First of all, with respect to CFATS, no one is more displeased than I am with some of the problems that have occurred there, and there is an action plan in place, there are changes in personnel among other things. And that program is going to run smoothly, and now the security plans are being evaluated, the tiering has occurred and the like.

Senator PRYOR. And there are lessons learned there?

Secretary NAPOLITANO. And there are lessons learned, as there are in all things. And this bill is less prescriptive than CFATS. First of all, this is a very regulation-like bill. This is a security bill. This is not a regulatory bill per se. But in terms just of management and organization, yes, there are some lessons learned from CFATS.

Senator PRYOR. Great. And I know that a lot of times when we read news media accounts about cybersecurity and even as we discuss it among ourselves, oftentimes we tend to focus on large companies and breaches that large companies experience. But the truth is a lot of small and mid-sized companies carry a lot of sensitive information. Is DHS working with small to mid-sized companies in any way to reach out to them to talk about best practices or anything like that?

Secretary NAPOLITANO. We conduct a lot of outreach activities with small and medium-size businesses on a whole host of cyber-related areas, so the answer is yes.

Senator PRYOR. Great. We always want to make sure that our small businesses are taken care of, and obviously if they are the weak link in the chain, that is a real problem.

Secretary NAPOLITANO. Well, Senator, as I continue to emphasize, when we are talking about the security of core critical infrastructure, if that goes down, a lot of these small businesses are dependent on that, and they will fail.

Senator PRYOR. Right. That is exactly right. Also, we often talk about the Federal Government, but also State governments have this same issue of cybersecurity, and obviously you are a former governor, former State Attorney General, as is the Chairman here, so you appreciate that State perspective. Are you working with States to try to talk about their best practices and lessons that you have learned?

Secretary NAPOLITANO. Yes, we are, and, indeed, we work with a multistate information system, and they are actually located or provide input into the NCCIC, the center that we talked about.

Senator PRYOR. Great. Mr. Chairman, that is all I have. I yield back the balance of my time. [Laughter.]

Chairman LIEBERMAN. Thank you, Senator Pryor. Next is Senator Carper.

Senator CARPER. Could I have his 14 seconds? [Laughter.]

Chairman LIEBERMAN. You got it.

OPENING STATEMENT OF SENATOR CARPER

Senator CARPER. Madam Secretary, good to see you. Good to see a former Secretary out there, a former governor out there, a former Congressman out there, Tom Ridge. Nice to see all of our witnesses. Thank you for being here.

One of the things, as my colleagues know, I like to do in hearings like this is to see if we cannot develop some consensus. You can never have too much of that in the Senate or in the House, and my hope is that when we adjourn here today we will have identified not just where we have differences, but we will have identified where we can actually find some common ground. So I will ask a couple of questions with that in mind.

I want to return to the comment of my colleague from Arizona who mentioned regulation, and with sort of a cautionary note, I just want to second what the Chairman said. Regulation can be a problem. It can be problematic. If we do not use common sense, if we do not look at cost/benefit analysis, it can be a bad thing.

Having said that, I always remember meeting with a bunch of utility chief executive officers (CEOs) 6 or 7 years ago, during my first term in the Senate, and they were meeting with me about clean air issues—sulfur dioxide, nitrous oxide, mercury, and carbon dioxide. And we were trying to decide what our path forward should be.

Finally, at the end of this meeting, the CEO from someplace down South, kind of curmudgeonly old guy, he said, "Look, Senator, just do this. Tell us what the rules are going to be, give us some flexibility, give us a reasonable amount of time, and get out of the way." That is what he said. And I have always remembered those words, and I think they may apply here today.

I want to thank the Chairman and our Ranking Member, Susan Collins, for calling our hearing and for working with me. The Chairman mentioned trying to open up, if you have an idea, bring it to us, and I think he has had an open door, and it is too bad that some have not taken full opportunity of that. But we have a lot of distractions around here, so sometimes that happens.

We all know we are being attacked by hackers from across the world and closer to home, and it is likely to get worse, not better.

And while some of the hackers are just there to cause mischief, some of them are there to steal ideas, steal our defense secrets, steal intellectual property, blackmail businesses and nonprofits, and to do worse.

The challenges that I think we have here, I think they really need a bold plan and we need a road map—I call it a "common sense road map"—to move forward. And I hope, again, that we can move along that way today.

I am especially pleased that the legislation that is being introduced includes a number of security measures that my staff and I have worked on with some of our colleagues for years to better protect our Federal information systems.

Having said that, I would like to begin, Madam Secretary, by asking you a couple of questions about the Department's efforts in this area, if I could.

As you know, I have been calling for some major changes to the laws that control how Federal agencies protect their information, our information systems. And when the Federal Financial Management, Government Information, Federal Services, and International Security Subcommittee that I chair first looked at this issue several years ago, we found that Federal agencies were wasting millions of dollars on reports that nobody read and hardly anybody understood and they did not make us any safer.

The bill that is before us today includes many improvements to the so-called Federal Information Security Management Act, affectionately known as FISMA, and that will ensure, we hope, our Federal agencies are actively monitoring and responding to threats, not just writing paper reports about them.

From what I understand, many agencies are already taking many steps to improve their security networks, largely because of the action you have taken in your Department to make FISMA more effective despite the outdated statute. I commend you for being proactive in this area and for putting forward a budget request that would ensure that your Department has the resources it needs to address this growing area of responsibility.

Can you describe some of the current limitations of FISMA for us and why this legislation and some of the new tools we give you just might be needed?

Secretary NAPOLITANO. Well, I think, just stepping back, one of the key things that this bill would do is by clarifying and centralizing where the authorities lie within the government and how those relate to the FISMA, among other things, so that it really sets, as you say, the common-sense road map for how we move forward.

You know, we have done a lot with the civilian networks of the government. As you know, they have been repeatedly and they are increasingly attempted to be infiltrated and intruded upon all the time. We have almost completed the deployment of what is known as EINSTEIN 2. We are working on the next iteration.

We have also in the President's budget request asked for a budget that would be held by the Department of Homeland Security but would be used to help improve or raise the level of IT protection within the civilian agencies.

Senator CARPER. All right. Thank you.

Just very quickly, if I could follow up just to get more specific, could you just talk a little bit more about what your Department will be able to achieve with what the President has requested, I think $200-some million for Federal network security, and how this legislation will impact those activities. You talked to it a little bit, but could you just drill down on that just a little for us?

Secretary NAPOLITANO. Right. And I can give you more detail on it, but basically what we will be able to do is have a fund out of which we can make sure that the civilian agencies of government are deploying best practices, hiring qualified personnel, in other ways strengthening their own cybersecurity within the Federal Government.

Senator CARPER. All right. Thanks.

Mr. Chairman, if I could just say in conclusion, one of the things that I hear a lot from businesses across the country and certainly in Delaware is they want us to provide for them certainty and predictability, and one of the things we are trying to do with this legislation and the regulations that may flow from it is just that, predictability and certainty. And with that in mind, I would say to our witnesses that are following, again, it would be really helpful if you all could figure out ways in your testimony not just to kind of divide us but help bring us together. That would be enormously helpful, not just to the Committee and to the Senate, but I think to our country. Thank you.

Chairman LIEBERMAN. Thank you, Senator Carper. Senator Levin.

OPENING STATEMENT OF SENATOR LEVIN

Senator LEVIN. Thank you very much, Mr. Chairman and our Ranking Member, for taking the initiative on this with other colleagues. Thank you, Madam Secretary, for all the work that the White House did on a similar bill which you had worked on, which I understand is basically part of now this pending bill which is on the calendar.

I am trying to understand what the objections are to the bill because it seems to me there is a whole bunch of protections in here for the private sector. As I have read at least a summary of the bill—and I have not read the bill yet—there is a self-certification or a third-party assessment of compliance with the performance requirements. I understand there is an appeal of those requirements if there is objection to it. I understand and believe that the owners of covered critical infrastructure that are in substantial compliance with the performance requirements are not liable for punitive damages which arise from an incident related to a cybersecurity risk.

So you have here something unusual, I believe, actually, for the private sector, which is a waiver of punitive damages. I do not know that it is unique, but I think it is fairly unique in legislation to waive the possibility of punitive damages in case of a liability claim.

There are a number of other protections in the privacy area, as I read the summary of this bill, for the information which must be provided where there is a significant threat which is identified. I am trying to identify—and I am not going to be able to stay to hear from the next panel as to what the objections are. I surely will read

the letter from the opponents and will study the bill that Senator McCain referred to. But I am trying to the best of my ability as we go along to see exactly what those objections are. There seems to be privacy protection here. There seems to be self-certification here which avoids part of a bureaucracy at least. There are limits on liability where there is a good-faith defense for cybersecurity activities, as the bill's heading says. There are a number of other protections.

I do not want you to argue for the people who have problems, obviously, but I would like you, to the best of your ability, to address what you understand are the key objections. We will hear them directly. We will read about them. But I think if you can, give us your response to them so we can have that for the record as well.

Secretary NAPOLITANO. Well, I think there are three kind of clusters. The first is that the bill is a regulatory bill, and it will be burdensome to industry to comply. And the answer is it is a security bill, not a regulatory bill. It really is designed with making sure we have a basic level of security in the cyber structures of our Nation's core critical infrastructure and that we have a way to exchange information that allows us to do that without private sector parties being afraid of violating other laws. And so this is not what one would consider a regulatory bill at all, and as Senator Collins said, it really is designed to protect the American economy, not to burden the American economy.

The second set of objections would, I think, revolve around the whole privacy area, but as the ACLU itself acknowledged, this bill really has done a very good job of incorporating those protections right from the get-go. And realize one of the reasons what DHS has the role it does is because we have a privacy office with a chief privacy officer who will be directly engaged in this. So the bill, I think, really addresses some of those privacy concerns.

And the third cluster would be—and I think Senator McCain kind of alluded to it—that it somehow duplicates the NSA. We do not need another NSA, and we do not need to clarify the authorities or the jurisdiction of the DHS. And I think there is a misconception there. The plain fact of the matter is, as the Chairman of the Joint Chiefs and Secretary Panetta and others have recognized, both the DOD and the DHS use the NSA, but we use it in different ways. So we are not duplicating or making a redundant NSA. We are taking the NSA and using it to the extent we can within the framework of the bill to protect our civilian cyber networks.

Senator LEVIN. And I understand that the Department of Defense basically supports this legislation. From what I can understand at least it does. Is that your understanding as well?

Secretary NAPOLITANO. I think not just basically. I think wholeheartedly.

Senator LEVIN. And in terms of the privacy concerns, those concerns are met with the privacy officer. But in terms of the information which is supplied where there has been a threat, that information when it is submitted to a government entity is protected.

Secretary NAPOLITANO. Right. The content is not shared. It is the fact of the intrusion——

Senator LEVIN. Tell us more about that protection.

Secretary NAPOLITANO. Yes, content is not shared. The information shared requires minimization. It requires elimination of personally identifiable information, all the things necessary to give the public confidence that their own personal communications are not being shared. So it is the fact of the intrusion, the methodology, the tactic used, the early warning indicators, all of those sorts of things are to be shared, but not the contents of the communication itself.

Senator LEVIN. Thank you. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks very much, Senator Levin. That was a really helpful exchange.

Senator Johnson.

OPENING STATEMENT OF SENATOR JOHNSON

Senator JOHNSON. Thank you, Mr. Chairman. Madam Secretary, nice to see you again.

First of all, I would like to say to Senator Lieberman and Senator Collins, I appreciate your work on this. This is, I think, critically important. It is also incredibly complex.

Is it appropriate for me to ask you a question, Mr. Chairman? I am new here. I do not want to be breaking protocol.

Chairman LIEBERMAN. I may have to consult my counsel, but go ahead.

Senator JOHNSON. You know, I share some of the concerns of Senator McCain, and because this is so important—it is certainly not a good way to start out the process. I mean, sort of in light of his objection and those of the other ranking members, are we going to consider not taking this to the floor directly or, I mean, is that going to be reconsidered on that basis?

Chairman LIEBERMAN. I do not believe so. I mean, I suppose if people want to raise the question, but I think there has been a long process here. Bills have been reported out of this Committee, out of Commerce, Intelligence, Foreign Relations had some stuff, all done—not all done on a bipartisan basis, but most of them were. Senator Reid got really agitated about this problem last year and began to convene the chairs and then held a joint meeting, which in these times is very unusual, a bipartisan meeting. Senator Reid and Senator McConnell urged the chairs and ranking members of all the committees to begin to work together to reconcile the differences. Some came to the table, as I said; some did not. We worked very hard to try to bring people in. I cannot speak for Senator Reid, but I think his intention is to take the bill that is the consensus bill now and bring it to the floor under his authority under Rule XIV, but to have a really open amendment process.

So I do not think anybody is going to rush this through, and there will be plenty of time for people to be involved. I am sure I speak for Senator Collins: We are open to any ideas anybody has.

Senator JOHNSON. I appreciate that. This is just really important to get right, so I would be concerned with that.

Chairman LIEBERMAN. I could not agree more. To me, the most important thing is to get it right, but also as quickly as we possibly can get it right, we should get it enacted.

Senator JOHNSON. OK.

Chairman LIEBERMAN. Because the crisis, the threat is out there. Senator Collins.

Senator COLLINS. Mr. Chairman, if I could just add one thing, and that is, this legislation has gone through a lot of iterations. It was reported first in 2010. I realize Senator Johnson was not part of the Committee at that point.

Senator JOHNSON. I am one of those new guys.

Senator COLLINS. But our staff has shared with the Senator's staff draft after draft after draft, invited them to briefings. I know the Senator has come to some of the classified briefings that we have had as well. So we have invited input from the Senator's staff.

Senator JOHNSON. Again, I am sincere in my appreciation of the work you are doing in this, and in a desire to get this right and move some legislation. So with that in mind, I know the House has worked on a bipartisan bill, H.R. 3523, which is just a very slimmed down version, probably an important first step, really trying to get information to be shared between the government and the private sector. Is that something you can support in case this thing gets all snagged up, maybe move toward something like that?

Secretary NAPOLITANO. Well, I would have to go back and look at that, but I think that there may be some parts of that are included within this bill. But this bill is a much stronger and more comprehensive focus on what we actually need in the cybersecurity area given the threats that are out there.

Senator JOHNSON. In terms of the carve-outs, I was talking to somebody who is far more knowledgeable about this than I am, and that was one of the big questions this individual expressed. If you are really trying to create cybersecurity, why would you carve out Internet Service Providers (ISPs), I mean, the people at the heart of it? It is kind of as if you are going to steal money, you go to the bank where it is. I mean, why would we carve out the service providers?

Secretary NAPOLITANO. I think from our standpoint, if you focus on the Nation's critical infrastructure and you really focus on the standards they have to meet, and you want to avoid some of the complexities that deal with like the ISPs and the like and where they are located and international jurisdiction, among other things, the carve-out is appropriate. In fact, it helps move the legislation along.

Senator JOHNSON. Have you done a cost assessment in terms of the cost of complying with these regulations?

Secretary NAPOLITANO. Well, I think talking about cost is important here. It is not our intent to have an undue cost on the core critical infrastructure of this country. It is, however, our belief that the costs of making sure you practice a common base level of cybersecurity, it should be a core competency within the Nation's critical infrastructure. And so while we do not want an undue cost, we do want a recognition that this is something that needs to be part of doing business.

Senator JOHNSON. Has there been an attempt to quantify that or will there be an attempt to quantify the cost of complying?

Secretary NAPOLITANO. I do not know. I would imagine, just thinking about it, that there will be many entities that already are at the right level. But, sadly, there are others that are not. And given that we are only talking about infrastructure that if intruded or attacked would have a really large impact on the economy, on

life and limb, on the national security, we are talking about a very narrow core part of the critical infrastructure. The fact that they all have to reach a base level is a fairly minimal requirement.

Senator JOHNSON. Just one last quick question. I am aware that the Chamber of Commerce is not for this bill, and the American Bankers Association. Do you have a list of private sector companies that have to comply with this that are in favor of it?

Secretary NAPOLITANO. Oh, there are a number of them, and I think they have been in contact with the Committee, but we can get that for you.

Senator JOHNSON. I appreciate that. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Johnson.

Secretary Napolitano, I appreciate your testimony very much. You made a really important point here, I think, first off that we define the group of owners and operators of private cyberspace in our country that are ultimately regulated here, that can be forced to meet the standards very narrowly, to include only those sectors which, if they were attacked, cyber attacked, would have devastating consequences on our society. So you are right. Obviously, it will cost some to enforce this, to carry it out, but it will be a fraction of what it would cost our society if there was a successful cyber attack. And I go back to the initial question. After 9/11, we just could not do enough to protect ourselves from another 9/11. And we have the opportunity here to do something preemptively, preventively, methodically, and at much less cost to our society overall.

Secretary NAPOLITANO. That is right, Mr. Chairman, and I think as you and I both noted, and I think Senator Collins did, in our opening statements, it is our responsibility to be proactive and not just reactive. We know enough now to chart a way ahead, and the bill does that.

Chairman LIEBERMAN. Yes, I agree. If we do not legislate, we do not create a system of protection of American cyberspace, and God forbid there is an attack, we are all going to be rushing around frantically to sort of throw money at the problem, and it is going to be after a lot of suffering that occurs as a result. So we have a real opportunity to work together. Nobody is saying this bill is perfect. I think it is very good after all it has been through. But the process continues. You have been very helpful today. I thank you very much, and we look forward to working with you. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. I, too, want to thank the Secretary for her excellent testimony and the technical assistance of the Department.

General Dempsey, Chairman of the Joint Chief of Staff, made a very clear statement at a hearing before the Armed Services Committee earlier this week. And General Dempsey said, "I want to mention for the record that we strongly support the Lieberman-Collins-Rockefeller legislation dealing with cybersecurity." So the Secretary's comment in response to the question of Senator Levin about where does the Department stands, when she said "wholeheartedly," is exactly right. And the Department testified to that effect.

Chairman LIEBERMAN. Thank you, Secretary Napolitano. Have a good rest of the day.

Senator NAPOLITANO. Thank you.

Chairman LIEBERMAN. We will call the final panel. Secretary Ridge is first. I know you are under a time pressure. I apologize for keeping you later than we had hoped, Secretary Ridge, but we have you, then Stewart Baker, James Lewis, and Scott Charney.

Gentlemen, thank you for your willingness to be here to testify and for your patience, although it got pretty interesting at times during the hearing, didn't it?

Secretary Ridge, in a comment that only you and I and two other people would appreciate, I do not think we will be going to the Common Man together tonight. That is another story.

Mr. RIDGE. I do not think so. But I would welcome the opportunity anytime you are ready.

Chairman LIEBERMAN. Thanks very much for being here. We will hear your testimony, and then we will understand if you have to go because I know you have another engagement and you are already late. Please proceed.

TESTIMONY OF HON. THOMAS J. RIDGE,[1] CHAIRMAN, NATIONAL SECURITY TASK FORCE, U.S. CHAMBER OF COMMERCE

Mr. RIDGE. Thank you very much. First of all, let me tell you what a pleasure it is to be back before the Committee. As I have told you before, my 12 years in the Congress of the United States I did enjoy being on that side of the table rather than this, but every time I have appeared before this Committee, the engagement has been civil, constructive, and substantive, and I hope I have been able to contribute. And I hope the fact that we agree in part and disagree in part today and there is significant agreement and disagreement does not preclude another invitation at another time. So it is a great pleasure to be before you.

I testify today on behalf of the U.S. Chamber of Commerce, which, as you well know, is the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, every sector, throughout every region in this country.

For the past year and a half, I have chaired the Chamber's National Security Task Force, which is responsible for the development and implementation of the Chamber's homeland and national security policies. And very much consistent with the President's concern, this Committee's concern, concerns on both sides of the aisle, you are probably not surprised that cybersecurity has been at the top of the list. When we have met with dozens and dozens of private sector companies and their vice presidents for security, be it bricks and mortar or cyber, this is very high, maybe at the top of their list right now.

So it is in my capacity as chairman but hopefully with a perspective also as the first Secretary of Homeland Security that I thank you for this opportunity to appear before you regarding cybersecurity and ways in which we can secure America's future.

[1] The prepared statement of Mr. Ridge appears in the Appendix on page 78.

At the very outset, Senator Lieberman and Senator Collins, one of the perspectives that I do want to share with you is that you need to add the Chamber of Commerce to the chorus of people sounding the alarm. They get it. And why do they get it? Because the infrastructure that we are worried about that protects America's national interest and supports the Federal, State, and local governments is the infrastructure that they operate. And in addition to being concerned about the impact of cyber invasion and incursion on their ability to do their job on behalf of the Federal Government, they also have 300 million consumers one way or the other they have to deal with.

So they join you, they join that chorus, not only in terms of the urgency of dealing with the threat, but I would dare say, and I say respectfully, they are probably better positioned to be able to calculate the consequences of systemic failure vis-a-vis a cyber attack than even an agency in the Federal Government. And on top of that, they have their interests to protect, fiduciary interests for shareholders if they are publicly traded. They have their employees. They have the communities they work in. They have the consumers. They have the suppliers. So we are in this together, and I think it is very important for you to understand that the Chamber joins the chorus that appreciates both the urgency of dealing with something, and I would say respectfully better understands from a macro level the horrific consequences to them and to their community and to their brand, their employees, and to this country from a significant cyber attack.

As you also know, the industry for years has been taking robust and proactive steps to protect and make their information networks more resilient. There has been much discussion with regard to process here, and let me just talk very briefly, and I am going to ask unanimous consent to get another minute or minute and a half, and I apologize for that. But as the first Secretary, I remember the national strategy that we created in 2002 talked about securing America, but we did not talk just about people, we did not just talk about bricks and mortar; we talked about cyber attacks as well.

In 2003, as has been referenced by Secretary Napolitano, the enabling legislation talked about cyber attacks as well. You move from the enabling legislation that creates the Department, and then you get Homeland Security Presidential Directive 7 (HSPD–7), and in anticipation of testifying I read what HSPD–7 says. It says, "Establish a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorists." It goes on to talk about protection from cyber attack as well.

In 2006, the National Infrastructure Protection Plan was established. The NIPP, updated in 2009, encompasses all that had gone on before to protect critical infrastructure and is specifically based on HSPD–7. The NIPP helped to create the Sector-Specific Agencies and the Sector Coordinating Councils—the point being that we do not need a piece of legislature, at least from the Chamber's point of view, that would identify and regulate critical infrastructure. We have been working on that for 10 years. It started with the enabling legislation, and you understand that process.

Where we tip the hat because compared to the first mark of the President's bill to this market, the information sharing, although we would probably like to tinker with it a little bit, is a vast improvement from the one that was initially placed and initially considered by the Administration. And, again, we are not ready to embrace it in its totality, but the concept, the direction, and the focus of it being bilateral we believe is the way to go.

So at the end of the day, with regard to covered critical infrastructure (CCI), there is really in our judgment no real need for that. We already have the process in place. People have been working together for 10 years, personal and institutional relationships to develop what that critical infrastructure is. You have cybersecurity experts in these Sector-Specific Agencies. So not only do you take a definition that appears to have no walls, ceilings, or floors, but it appears to be redundant.

And, second, it does—somebody used the word "requirements." And one of the great concerns we have is that requirements and prescriptions are mandates, mandates are regulations, and, frankly, the attackers and the technology moves a lot faster than any regulatory body or political body will ever be able to move.

So, in my judgment—and, again, we need to talk—the Chamber agrees. The sections in here with regard to the international component, the public awareness component, the FISMA component, and some of the others, we applaud and celebrate. And hopefully if you tied those together, if you are looking to really deal with this in an immediate way as quickly as possible with a more robust information-sharing proposal, marry it with the House and then you will have that bipartisan agreement.

So I was hurried. I appreciate and respectfully request that my full statement be included as part of the record, and thank you for the opportunity of appearing before you.

Chairman LIEBERMAN. Thanks, Mr. Secretary, and we will definitely include your statement in full in the record.

Am I right that you have to leave?

Mr. RIDGE. You were, but I think it is a little too late. I appreciate that.

Chairman LIEBERMAN. Can you stay?

Mr. RIDGE. I am prepared to stay to answer questions. I can leave at 6 o'clock instead of 5 o'clock. I have to be on a plane—but thank you for asking.

Chairman LIEBERMAN. Do you want us to ask you a few questions now and then have you go? Or with the sufferance of the——

Mr. RIDGE. I think that in deference, it is a little late to get there, so I appreciate that.

Chairman LIEBERMAN. I am going to yield to Senator Collins, and if there is anything left to ask when she is done—— [Laughter.]

Senator COLLINS. Thank you, Mr. Chairman.

First, Secretary Ridge, as you know, I have the greatest respect and affection for you personally and the greatest respect for the Chamber of Commerce, which is why I am disappointed that we do not see this issue exactly in the same way.

I would also note a certain irony since the Chamber itself was under cyber attack by a group of sophisticated Chinese hackers for

some 6 months at least, during which time the hackers had access to apparently everything in the Chamber's system, and the Chamber was not even aware of the attack until the FBI alerted the Chamber in May 2010. So there is a little bit of irony, but I will assure you that under our bill the Chamber is not considered critical infrastructure. [Laughter.]

Mr. RIDGE. But Senator, you raise a very interesting point, and I guess the question I have, if it is not critical infrastructure but a significant organization representing the critical economic infrastructure of America, why in the world did the FBI delay informing the organization that represents the economic infrastructure of America? Somebody ought to ask that question. Frankly, I have heard some cases where people in the private sector have reported potential—this has not been verified—incidents to the Federal Government and they said, "We knew." What do you mean you knew?

Senator COLLINS. Well, that is one reason——

Mr. RIDGE. You cure some of that problem.

Senator COLLINS. I was just going to point to that. We have very robust information-sharing provisions in our bill that will cure that very problem.

But the fact is, in drafting this latest version of our bill, we have taken to heart many of the concerns raised by the Chamber, and, thus, just to clarify exactly where the Chamber is on these issues, I do want to ask your opinion on some of the changes that we have made in direct response to the Chamber's concerns.

For example, we now have a provision that says that entities that are already regulated by existing regulations would be eligible for waivers and entities able to prove that they are sufficiently secure would be exempted from most of the requirements under this bill. The bill would require the use of existing cybersecurity requirements and current regulators.

Does the Chamber support those changes that were incorporated in response to the Chamber's concerns?

Mr. RIDGE. Well, I think you have incorporated several changes, Senator Collins, and I cannot speak directly, but I believe that is one of them. And I think it also goes to the point, however, that some of that oversight is being done within the existing process and protocol, and with the dramatic potential changes in information sharing, it is a system that will work.

One of the questions I had when I listened to the chorus of people who support the bill, I just wondered if the Secretary of Defense believes that the Defense Industrial Base likes the cyber model of information sharing that was announced by the Department of Defense in June 2011 or they would prefer to be regulated. I think there are some unanswered questions here.

But I think the point that I want to be very strong about, Senator Collins, is that you have heard some of the concerns, and we are grateful for that.

Senator COLLINS. Well, that is my point as we, frankly, have bent over backwards to try to listen to legitimate concerns without weakening the bill to the point where it can no longer accomplish the goal.

Another important provision of the bill is that the owners of critical infrastructure, not the government, not DHS, would select and

implement the cybersecurity measures that they determine are best suited to satisfy the risk-based performance requirements. Does the Chamber support having the owners of the infrastructure decide rather than government mandating specific measures?

Mr. RIDGE. Well, I think, again, if I recall and interpret your legislation correctly, the Chamber likes the notion and embraces the notion that the Sector-Specific Agencies, the respective departments and agencies who have the Sector Coordinating Councils, have been working on identifying critical infrastructure and sharing the kind of information that we think is necessary to not immunize us completely because the technology and the hacking procedures are going to change, but to dramatically reduce the risk. In fact, it is in everybody's interest, particularly the owners, to move as quickly as possible.

The logic that has been applied to relieving, I guess, Cisco, Microsoft, and others so they can move adroitly and respond to the risk seems to me would be pretty decent logic to apply to everybody else in the economy as well who do not want to be burdened by a series of regulations or prescriptive requirements.

Senator COLLINS. Well, since the private sector under our bill is specifically involved in creating the standards, I do not see how that produces burdensome standards since the Secretary has to choose from the standards that the private sector develops. Again, another change that we strengthened in our bill.

Another question that I would have for you, I assume that the Chamber supports the liability protections that are included in this bill, so that if a company abides by the performance standards and there is an attack anyway, the company is immune from punitive damages.

Mr. RIDGE. Well, they have not tapped me on the shoulder, but I presume they do.

Senator COLLINS. Well, in back of you a young woman is nodding vigorously.

Mr. RIDGE. I presume they do. If I were the Chamber, I would certainly encourage them to embrace that wholeheartedly.

Senator COLLINS. Well, my time has expired, but my point is that there are many provisions in this bill that we changed in direct response to input from the Chamber, and I would like the Chamber to acknowledge that.

There is one final point that I want to make. When you were talking about that CEOs are invested in cybersecurity because of the impact on their customers and their clients, and so it is in their own self-interest, I cannot tell you how many chief information officers (CIOs) with whom I have talked who have told me, "If only I could get the attention of the CEO on cybersecurity. We are not investing enough, we are not protecting our systems enough, and it is just not a priority for the CEO."

So I would suggest to you to talk to some CIOs because I think you would get a totally different picture.

Mr. RIDGE. Well, I appreciate that, Senator Collins. You know, I am familiar with quite a few major companies in America and what they are doing with regard to cyber, and my experience is 180 from yours. I realize that there are probably some people out there—I do not imagine too many organizations—and anybody in

an organization would like a little bit more money to enhance their capability to safeguard or to manage the risk. But I will take you at your word that there may be some CIOs who feel very strongly and have reflected that in their statements to you.

I think at the end of the day, though, I think you have made a valuable contribution. You have listened to the Chamber. We applaud those things we agree with, and we are just going to respectfully disagree that you are going down the path very similar to what we are concerned about, a prescriptive regimen. I notice some of the literature talks about a light touch, but a light touch can turn into a stranglehold if it goes too far down the process. And if you take a look at the Chemical Facility Anti-Terrorism Standards, what was to be a light touch may become very prescriptive, because once the legislation was passed, there were Members of Congress, your colleagues, who said, well, that is not enough and we may need very specific technology and we need very specific regulations.

So, again, it is that slippery slope that I think they are most concerned about, and I very much appreciate you giving me a chance to articulate it before the Committee.

Senator COLLINS. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Collins.

I have no further questions, Secretary. Thanks for being here. We are glad to liberate you to catch the next plane.

Mr. RIDGE. Well, you are very kind. I thank you. It has been my great pleasure, and as I said before, I look forward to future opportunities, in the "what it is worth" department, to share my thoughts with this Committee. I thank my friends.

Chairman LIEBERMAN. We do, too.

Mr. RIDGE. Senator Akaka, best wishes to you, sir. Thank you.

Chairman LIEBERMAN. Thank you.

Stewart Baker is our next witness, currently a partner in the law firm of Steptoe and Johnson, former General Counsel for the much mentioned today NSA from 1992 to 1994 and Assistant Secretary at DHS from 2005 to 2009 during which time we benefited greatly from your counsel and service. Thanks for being here, and we would welcome your testimony now.

TESTIMONY OF HON. STEWART A. BAKER,[1] PARTNER, STEPTOE AND JOHNSON LLP

Mr. BAKER. It is a great pleasure. Thank you, Chairman Lieberman, Senator Collins, and Senator Akaka. It is a nostalgic moment to come back here, and I want to congratulate you on your achievement in moving this bill in a comprehensive form as far as it has gone. It is a very valuable contribution to our security.

I just have two points, but before I do that, I thought I would address the Stop Online Piracy Act analogy, the idea that this is like SOPA and the Internet will rise up to strike it down.

I am proud to say, if I can channel Senator Lloyd Bentsen for a minute, I knew SOPA, I fought SOPA, and, Mr. Chairman, this bill is no SOPA. [Laughter.]

Chairman LIEBERMAN. Hear, hear.

[1] The prepared statement of Mr. Baker appears in the Appendix on page 83.

Mr. BAKER. In fact, I opposed SOPA for the same reason that I support this bill. As a Nation, as a legislature, our first obligation is to protect the security of this country. SOPA would have made us less secure, to serve the interests of Hollywood. This bill will make us more secure, and that is why I support it.

Just two points on why I believe that. We know today the most sophisticated security companies in the country have been unable to protect their most important secrets. This shows us how deep the security problem runs. We also know from direct experience, things that I saw when I was at DHS and that have emerged since, that once you penetrate a network, you can break it in ways that leave behind permanent damage. You can break industrial control systems on which refineries, pipelines, the power grid, water, and sewage all depend. And we have had a lot of analogies today about how this is like September 10, 2001. If you want to know what it would be like to live through an event where someone launches an attack like this, the best analogy is New Orleans, the day after Hurricane Katrina hit. You would have no power; you would have no communications. But you also would not have had the warning and the evacuation of most of the city's population, and you would not have the National Guard in some safe place, ready to relieve the suffering. It could, indeed, be a real disaster, and we have to do something to protect against that possibility. That is not something the private sector can do on its own. They are not built to stand up to the militaries of half a dozen countries, and that is why it is important for there to be a government role here.

I do think that with this bill—in contrast to the views of the Chamber—you may have gone a little far in accommodating them, and I will just address one point that I think is particularly of concern.

I fully support the idea that there should be a set of performance requirements driven by the private sector, implemented by the private sector, and with private sector flexibility to meet them as they wish. But the process of getting to that and then getting enforcement is time-consuming. It could take 8 years; it could take 10 years if there is resistance from industry or a particular sector. And it may be worth it to take that time to get standards that really are something that the private sector buys into and is willing to live with. But I think we have to recognize that in the next 8 to 10 years we could have an attack. We could have an incident. We could have some very serious trouble or a threat that requires that we move faster than that statutory framework would suggest.

And so I would suggest that if there is one change that I would make to this bill, it is to put in a provision that says that in an emergency, where there really is an immediate threat to life and limb, the Secretary has the ability to compress all of the time frames and to move quickly from stage to stage so that if we only have a week to get the grid protected, she is in a position to tell the power companies, "You will be here on Tuesday and bring your best practices because by Friday you are going to have to start implementing them because we know there is an attack coming this week." That is something that we need to be able to do and to have the flexibility to do. Thank you.

Chairman LIEBERMAN. Very helpful. Thank you very much. We will talk more about that.

Dr. Jim Lewis, thanks for being here. He is Director and Senior Fellow of the Technology and Public Policy Program at the Center for Strategic and International Studies. Dr. Lewis was also the Director of the CSIS Commission on Cybersecurity, which began its work in 2008. Thanks so much. Please proceed.

TESTIMONY OF JAMES A. LEWIS, PH.D.,[1] DIRECTOR AND SENIOR FELLOW, TECHNOLOGY AND PUBLIC POLICY PROGRAM, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you, Senators, for giving me the opportunity to testify. You know, when we hear that getting incentives right and letting the private sector lead or sharing more information will secure the Nation, remember that we have spent the last 15 years repeatedly proving that this does not work, and from an attacker's perspective, America is a big, slow target.

Some people say the threat is exaggerated. This is really unfortunate. You have talked about the parallels with September 11, 2001. But in some ways we are on a path to repeat the September 11 error if we do not take action in the very near term.

The threat is real and growing. Military and intelligence services with advanced cyber capabilities can penetrate any corporate network with ease. Cyber criminals and government-sponsored hackers routinely penetrate corporate networks. And new attackers, ranging from Iran and North Korea to a host of anti-government groups, are steadily increasing their skills.

The intersection of greatest risk and weakest authority is critical infrastructure. National security requires holding critical infrastructure to a higher standard than the market will produce.

This bill has many useful sections on education, research, securing government networks, and international cooperation, and they all deserve support. But the main event is regulating critical infrastructure for better cybersecurity. Without this, everything else is an ornament, and America will remain vulnerable. Low-hanging fruit will not make us safer, and one way to think about this is if you took the section on critical infrastructure regulation out of this bill, it would be like a car without an engine. So I look forward to what we will see next week.

There are all sorts of objections to moving ahead. We heard that innovation could be damaged, but well-designed regulation will actually increase innovation. Companies will innovate at making safer products. We have this with Federal regulation of cars, airplanes, even as far back as steamboats. Regulation can incentivize innovation.

Everyone agrees that we want to avoid burdensome regulation and focus new authorities on truly critical systems. The bill as drafted takes a minimalist and innovative approach to regulation based on commercial practices, so I appreciate the effort that has gone into that.

Many in Congress recognize the need for legislation, and this Committee, the Senate, and others in the House deserve our

[1] The prepared statement of Mr. Lewis appears in the Appendix on page 92.

thanks for taking up this task. But the battle has shifted. People will try to dilute legislation. They will try to put forward slogans instead of solutions, and they will write in loopholes. The goal should be to strengthen not to dilute, and so two problems need attention.

The first is the threshold for designating controlled critical infrastructure. Cyber attacks in the next few years are most likely to be targeted and precise. They probably will not cause mass casualties or catastrophic disruption. If we set the threshold too high, it is simply telling our attackers what they should hit. So we need to very carefully limit the scope of this regulation, but I fear that we may have gone a bit too far.

The second is the carve-out for commercial information technology, and others have raised this. It makes sense that industry does not want government telling them how to make their products. That is perfectly reasonable. But a blanket exemption on services, maintenance, installation, and repair would, first, undo central work started by the Bush Administration; and, second, leave America open for a Stuxnet-like attack. So these parts of the bill should really be removed, and in particular, I would call your attention to paragraph (A) and (B) of Section 104(b)(2).

In any important legislation, there is a delicate balance between protecting the Nation and minimizing the burdens on our economy. This bill, with some strengthening, I think can achieve that balance and best serve the national interest. The alternative is to wait for the inevitable attack. My motto for 2012 in cybersecurity is, "Brace for impact."

I thank the Committee and will be happy to take any questions.

Chairman LIEBERMAN. Thank you, Dr. Lewis. Your voice is an important one to listen to, and we will, we do.

Scott Charney is our last witness today. He is the Corporate Vice President of the Trustworthy Computing Group—that is a good job—at Microsoft Corporation. Thanks for being here.

TESTIMONY OF SCOTT CHARNEY,[1] CORPORATE VICE PRESIDENT, TRUSTWORTHY COMPUTING GROUP, MICROSOFT CORPORATION

Mr. CHARNEY. Chairman Lieberman, Senator Akaka, thank you for the opportunity to appear at this important hearing on cybersecurity. In addition to my role as Corporate Vice President for Trustworthy Computing, I serve on the President's National Security Telecommunications Advisory Committee and was Co-chair of the CSIS Commission on Cybersecurity for the 44th Presidency.

Microsoft has a long history of focusing on cybersecurity. In 2002, Bill Gates launched our Trustworthy Computing Initiative. As we celebrate the 10th anniversary of that effort, we are proud of both our progress and conscious of how much work remains to be done. While IT companies are providing better cybersecurity, the world is increasingly reliant on cyber-based systems, and those attacking such systems have increased in both number and sophistication. Cyber attacks represent one of the more significant and complex threats facing our Nation.

[1] The prepared statement of Mr. Charney appears in the Appendix on page 99.

With that in mind, I commend the Chairman, the Ranking Member, this Committee, and Members of the Senate for your continuing commitment to addressing cybersecurity. We appreciate your leadership in developing the legislation that was introduced earlier this week. Over the past few years, you have helped focus national attention on this urgent problem, offered constructive proposals, and conducted an open and transparent process to solicit the views of interested private sector stakeholders.

Microsoft believes the current legislative proposal provides an appropriate framework to improve the security of government and critical infrastructure systems and establishes an appropriate security baseline to address current threats. Furthermore, the framework is flexible enough to permit future improvements to security, an important point since security threats evolve over time.

While the Internet has created unprecedented opportunities for social and commercial interaction, it has also created unprecedented opportunities for those bent on attacking IT systems. Securing IT systems remains challenging, and it is important that legislative efforts designed to improve computer security meet three important requirements:

First, legislation must embrace sound risk management principles and recognize that the private sector is best positioned to protect private sector assets. Second, the legislation must enable effective information sharing among government and industry members. Third, any legislation must take into account the realities of today's global IT environment. I will discuss each of these important issues in turn.

First, sound risk management principles require that security efforts be directed where the risk is greatest and that those responsible for protecting systems have the flexibility to respond to ever changing threats. To ensure that this happens, it is important that the definition of critical infrastructure be scoped appropriately and that the owner of an IT system ultimately be responsible for developing and implementing security measures. We believe that the current legislation, which allows the government to define outcomes but allows the private sector owner of a critical system or asset to select and implement particular measures, is the right framework.

Second, successful risk management depends on effective information sharing. For too long, people have cited information sharing as a "goal" when, in fact, it is a tool. The goal should not be to share all information with all parties, but rather the right information with the right parties, that is, parties who are positioned to take meaningful action. We appreciate that this legislation attempts to remove barriers to information sharing by specifically authorizing certain disclosures and protecting the information shared.

Finally, as a global business, we are very cognizant of the fact that countries around the world are grappling with similar cybersecurity challenges and implementing their own cybersecurity strategies. We believe that actions taken by the U.S. Government may have ramifications beyond our borders, and it is important that the United States lead by example, adopting policies that are technology neutral and do not stifle innovation. It must also promote

cyber norms through international discussions with other governments.

Unlike some traditional international efforts where government-to-government discussions may suffice to achieve desired outcomes, it must be remembered that the private sector is designing, deploying, and maintaining most of our critical infrastructures. As such, the United States needs to ensure that the owners, operators, and vendors that make cyberspace possible are part of any international discussions.

I would note in closing that security remains a journey, not a destination. In leading our Trustworthy Computing effort over the last 10 years, I have witnessed the continual evolution of Microsoft's own security strategies. Technologies advance, threats change, hackers grow stronger, but defenders grow wiser and more agile. The Committee's legislation, which focuses on outcomes and ensures meaningful input by the private sector, represents an important step forward. Microsoft is committed to working with Congress and the Administration to help ensure this legislation meets these important objectives while minimizing unintended consequences.

Thank you for the leadership that you have shown in developing this legislation under consideration today and for the opportunity to testify. I look forward to your questions.

Chairman LIEBERMAN. Thanks very much to you, too, Mr. Charney.

Let me ask all three of you a threshold question, no pun intended. As you can hear from some of the testimony and some of the questions from Committee Members, there is a question still about whether regulation is necessary here—I am using a pejorative term. Let me just say government involvement here is necessary. And at its purest, this argument is that obviously the private sector that owns and operates cyber infrastructure has its own set of incentives to protect itself. Why do we need the government to be involved? Mr. Baker, do you want to start?

Mr. BAKER. Sure. It seems to me that, fundamentally, the private sector and each private company has an incentive to spend about as much on security as is necessary to protect their revenue streams, to prevent criminals from stealing things from them and the like. It is much less likely that they are going to spend money to protect against disasters that might fall on someone else, on their customers down the road, that are unpredictable. And so there are certain kinds of harms, especially if you are in a business where it is hard for people to steal money from you but it is easy for them to change your code in a way that could later be disastrous for consumers. That is a situation businesses will view as something that they are not ever going to get a higher payment for addressing when they sell their products and, therefore, not something that they would want to spend a lot of money on.

So it does seem to me that there are a lot of externalities here that require the government to be involved in addition to the problem that if you are the Baltimore Gas and Electric company, for example, you really do not know how to deal with an attack launched by Russian intelligence.

Chairman LIEBERMAN. Right. Dr. Lewis.

Mr. LEWIS. Thank you. Sometimes I call them "mandatory standards," and that is nicer than "regulation," but I wanted to say "regulation" this time because we have to put it out on the table.

Chairman LIEBERMAN. Right.

Mr. LEWIS. We got the incentives wrong in 1998, the first time we thought about protecting critical infrastructure. We thought that if you tell them about the threat, get them together, share a little information, and they will do the right thing. And as you have heard, the return on investment is such that companies will spend up to a certain level. It is not even clear that all of them do that, by the way, but they will not spend enough to protect the Nation.

So we are stuck with a classic case of a public good, national defense regulation is essential, and if we do not regulate, we will fail.

Chairman LIEBERMAN. Let me just follow up. You made a statement in your opening remarks—I am going to paraphrase it—which is that a hostile party, a nation state, or intelligence agency could penetrate any entity's cyberspace in this country if they wanted. Did I hear you right?

Mr. LEWIS. You did. The full answer is complicated, so I will be happy to provide it to you in writing. But when you think of the high-end opponents who can use a multitude of tactics, including tapping your phone line, including hiring agents or corrupting employees, these are very hard people to stop. And the assumption that is probably safest to make from a defensive point of view is that all networks have been compromised.

Chairman LIEBERMAN. Mr. Charney.

Mr. CHARNEY. I would say two things. First, I would echo what Mr. Baker said. I think market forces are actually doing a very good job of providing security. The challenge is market forces are not designed to respond to national security threats. You cannot make a market case for the Cold War. And so you really have to think about what will the market give us? What does national security require? And how do you fill the delta between those gaps?

The second thing I would say about looking at regulating critical infrastructure, is in my 10 years at Microsoft, I have found as we have struggled with cybersecurity strategies, we really live in one of three states of play. Sometimes we do not know what to do, and you have to figure out a strategy. Sometimes you know what to do, but you are not executing very well, in which case you need to go execute better. Sometimes we know what to do and we execute well, but we do not execute at scale.

I think there are some companies that do a very good job of protecting critical infrastructure today. Are we doing it at enough scale to really manage the risk that the country faces? And I do not think we are today, and that is why in our report of the CSIS Commission and in my testimony we are supportive of the framework that has been articulated in the legislation.

Chairman LIEBERMAN. I appreciate that. Assuming the statistics are accurate or close to accurate about the frequency of intrusion into cyberspace owned and operated in the private sector, then that makes it self-evident that there is not enough being done to protect from that.

Dr. Lewis, let me ask you something. You offered a friendly criticism of the bill just before, which is that our definition of "covered critical infrastructure" is too narrow, too high. We are limiting it too much. Give me an idea about how you might broaden it if you were drafting the legislation.

Mr. LEWIS. I think we are talking about relatively simple amendments to the language, Mr. Chairman. I would look at some of the thresholds you have put in: Mass casualties. What is a mass casualty event? For those of us coming out of the Cold War, that was a very high threshold. Economic disruption on a catastrophic scale—it is not clear to me that Hurricane Katrina, for example, would be caught by that definition. So I think it is more an issue of clarifying, more an issue of making sure that the smaller attacks that we are more likely to see in the near future are caught by this threshold and we are not just looking for the big bang.

Chairman LIEBERMAN. Thanks. My time is up. Senator Akaka, thank you for being here.

OPENING STATEMENT OF SENATOR AKAKA

Senator AKAKA. Thank you very much, Mr. Chairman, for holding this hearing. I applaud your tenacity and that of Senators Collins, Rockefeller, and Feinstein in pursuing the comprehensive cybersecurity legislation we are considering today. I also want to thank you and the Administration for incorporating my suggestions to the cyber workforce provisions of the bill. Employees of the Department of Homeland Security are on the front lines of countering the cyber threat, and we must make sure the Department has the appropriate tools to attract and retain the workforce it needs to meet these complex challenges.

Stakeholders have raised concerns about the privacy and civil liberties implications of certain provisions of this bill. I want to commend the bill's authors for making progress in addressing these concerns. It is important for the final product to adequately protect Americans' reasonable expectation of privacy, and I will continue to closely monitor this issue.

FBI Director Robert Mueller's recent statement that the danger of cyber attacks will equal or surpass the danger of terrorism in the foreseeable future is a stark reminder that strengthening cybersecurity must be a key priority for this Congress. Cyber criminals and terrorists are targeting our critical infrastructure, including our electricity grids, financial markets, and transportation networks, and these have been mentioned by the panelists. American businesses face constant cyber attacks that seek to steal their intellectual property and trade secrets. However, cybersecurity policy has been slow to adjust to these ever increasing and sophisticated cyber threats.

The Cybersecurity Act of 2012 will give the Federal Government and the private sector the tools necessary to respond to these troubling threats, I feel. Finalizing this important legislation is a pressing priority for this Congress, and I look forward to working with you on this.

As you know, the bill contains new hiring and pay authorities to bolster the Federal civilian cybersecurity workforce. It also has provisions to educate and train the next generation of Federal cyberse-

curity professionals. I would like to hear your views on the challenges of recruiting and retaining cybersecurity professionals, the provisions in this bill, and any other recommendations you may have to address these growing workforce challenges. Mr. Baker.

Mr. BAKER. If I might, I would like to just defer to Mr. Charney, who really has more expertise and experience in this field, and if there is anything else, I will add to it after.

Senator AKAKA. Fine. Mr. Charney.

Mr. CHARNEY. It is very challenging to find well-trained cybersecurity professionals even in the private sector. This technology has just proliferated far faster than educational institutions could educate people to manage IT security and manage the security.

As a result of that, Microsoft has actually committed considerable resources, supporting programs like science, technology, engineering, and mathematics (STEM) education, or Elevate America where we provided over a million vouchers for entry-level and more advanced computer basic skills. But it is a big challenge, and if it is a big challenge for the private sector, you can imagine that it would also be a large challenge for the public sector as they do not have the same pay scale that I have available to me.

So this is a big challenge. It is a challenge in both education and in proficiency of the workforce. And, in fact, the CSIS Commission issued a report on the challenges of getting an educated, cyber-educated workforce.

Mr. BAKER. And I would just add to that, indeed, that DHS has had particular difficulty in attracting people and working through their personnel hiring procedures. Anything that makes that smoother and more responsive to the market is useful.

But finally, and most importantly, for every student who is watching this wondering what he is going to do when he graduates from college, these jobs are waiting for you. You owe it to your country and you owe it to yourself to pursue these opportunities.

Senator AKAKA. Thank you. Mr. Lewis.

Mr. LEWIS. Senator, 2 years ago, at the end of July, CSIS had an event here on the Hill, on education for cybersecurity, and I was kicking myself because I thought no one is going to be here on July 29. It is just stupid. And so I told them, "Cut back on the food. We do not need it." And we had standing room only. They had to put chairs in the hall. People love this topic, but there are a couple of issues to think about.

On the government side, we need to have a clearer career path for people to get promoted up.

On the private sector side, the education that we get now needs to be refined and focused. A degree in computer science may not give you the skills. In fact, it probably will not give you the skills for cybersecurity. And so some of the provisions in the bill such as the cyber challenge, and other programs, tap into this real enthusiasm among teenagers and among college students to get into this new field. And I think this is one of the stronger parts. Again, doing the education piece is important, but it will not protect us in the next few years, which is why we need the other parts of the bill as well.

Senator AKAKA. Thank you very much, panel. My time has expired, Mr. Chairman.

Chairman LIEBERMAN. Thanks, Senator Akaka, and thanks very much for the contribution you made to the bill, as indicated by your questioning, on the cyber workforce. That was very important.

Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman. The hour is late, but I just want to thank our witnesses for their excellent testimony. Hearing some of our witnesses on this panel raise some legitimate questions about whether we have gone too far in trying to accommodate concerns raised by the Chamber and other groups makes me think that maybe we have gotten it just right since the Chamber is still not happy and you believe we have gone too far.

But in all seriousness, your expertise has been extremely helpful, as has the input that we have had from Microsoft, from the Chamber, from the tech industry, and from experts and academics. We really have consulted very widely, and it has been very helpful to us as we try to strike the right balance.

This is an enormously important but complicated, complex issue for us to tackle, but tackle it we must. And that is something that I believe unites all of the witnesses from whom we have heard today.

Whether we consider this to be a response to a 9/11-like attack or a Hurricane Katrina, I just do not want us to be here after a major cyber incident saying, "If only, and how could we have ignored all these warnings, all these commissions, all of these studies, all of these experts?" I cannot think of another area in homeland security where the threat is greater and we have done less.

There is a huge gap. Whether we got it exactly right on chemical plant security, port security, or reform of the Federal Emergency Management Agency, at least we acted and we have made a difference in each of those areas. They are not perfect, but we have acted and we have made a difference. And in intelligence reform, I think we have made a big difference.

But here we have a vulnerability, a threat that is not theoretical. It is happening each and every day, and yet we have seen today by the comments of some of our colleagues this is going to be a very difficult job to get this bill through. I am confident that we can do it, however, and that in the end we will succeed.

And, finally, I do want to say to our colleagues, to those who are listening, to those in the audience, that we need your help. If you have other good ideas for us, by all means bring them forward. Help us get the best possible bill. But for anyone to stand in the way and cause us to fail to act at all to pass legislation this year I think would just be a travesty. It would be a disaster waiting to happen for our country.

So, Mr. Chairman, I would just encourage you to press forward, and I will be at your side, your partner, all along the way. We have done it before against great odds.

Chairman LIEBERMAN. And we will do it again. Hear, hear. Thank you. That meant a lot to me, and it is just expressive and characteristic of your independence of spirit and your commitment to do what you think is right for our national security.

We are going to press forward, and the Majority Leader, Senator Reid, I am confident is going to press forward, too. As I mentioned earlier, he had a couple of briefings on this problem of cybersecu-

rity last year, and it really troubled him. He feels that there is a clear and present danger to our national security and our economic prosperity from cyber attack. That is why he has devoted a lot of time to trying to get us to this point that we have reached this week to have at least a foundational consensus bill and why I am confident he is going to bring this to the floor with the authority he has as Majority Leader. I am optimistic that may well be in the next work period, which is when we come back at the end of February and into March.

The three of you have added immensely to our work here. I do want to continue to work—I do not want to ask a question because Senator Collins has brought this to such a wonderful ending point, but I do want to, over time as we take the bill to the floor, invite you—particularly Mr. Baker and Dr. Lewis, who have expressed concerns about the so-called carve-out. People in the Administration still think that with the authority that we have left in there, the language will allow the government to develop performance standards that will require owners of systems to protect those systems even if they might include some commercial products. But we hear your concerns, and we invite you to submit thoughts to us as to how to do this better, and we promise we will consider those concerns.

Any last words from any of the three of you?

[No response.]

Chairman LIEBERMAN. Thanks very much for all you have contributed. I thank Senator Collins again. It is true, we get very stubborn, the two of us, when we think something is really right and necessary. So we are going to plow forward.

The record of this hearing will be held open for 10 days for any additional questions or statements for the record. I thank you again very much.

With that, the hearing is adjourned.

[Whereupon, at 5:20 p.m., the Committee was adjourned.]

APPENDIX

United States Senate
Committee on Homeland Security and Governmental Affairs
Chairman Joseph I. Lieberman, ID-Conn.

Opening Statement of Chairman Joseph Lieberman
"Securing America's Future: The Cybersecurity Act of 2012"
Homeland Security and Governmental Affairs Committee
February 16, 2012

The hearing will come to order, good afternoon. This is the 100th hearing our Committee has held on cybersecurity and I hope it is the last before the comprehensive cybersecurity bill before us today is enacted into law.

The fact is that time is not on our side.

To me it feels like Sept. 10, 2001. The question is whether we will act to prevent a cyber 9/11 before it happens instead of reacting after it happens.

The reason for this legislation is based in fact. Every day rival nations, terrorist groups, criminal syndicates and individual hackers probe the weaknesses in our most critical computer networks, seeking to steal government and industrial secrets or to plant cyber agents in the cyber systems that control our most critical infrastructure and would enable an enemy to seize control of a city's electric grid or water supply system with the touch of a key from a world away.

The current ongoing and growing cyber threat not only threatens our security here at home, but it is right now having a very damaging impact on our economic prosperity. Extremely valuable intellectual property is being stolen regularly by cyber exploitation by people and individuals and groups and countries abroad. It is then being replicated without the initial cost done by American companies. This means jobs are being created abroad that would otherwise be created here.

So when we talk about cybersecurity, people naturally focus on the very real danger that an enemy will attack us through cyberspace, but as we think about how to grow our economy and create jobs again, I've come to the conclusion this is one of the more important things we can do to protect the treasures of America's intellectual innovation from being stolen by competitors abroad.

Last year a very distinguished group of security experts, led by former Department of Homeland Security Secretary Mike Chertoff and Defense Secretary Bill Perry issued a stark warning:

"The constant assault of cyber assaults has inflicted severe damage to our national and economic security, as well as to the property of individual citizens. The threat is only going to get worse. Inaction is not an acceptable action." I agree.

340 Dirksen Senate Office Building, Washington, D.C. 20510
Tel. (202) 224-2627 Web: http://hsgac.senate.gov

The bill before us today is the product of hard work both across party lines and committee jurisdictional lines. I particularly want to thank my colleagues Senator Collins and Commerce Secretary Jay Rockefeller and Intelligence Committee Chairman Dianne Feinstein for all their hard and cooperative work in getting us to this point. We're going to be privileged to hear from all three of them shortly.

I also want to thank Senator Carper for his significant leadership contributions to this effort.

And I want to thank the witnesses who are here. We've chosen the witnesses deliberately because they hold differing points of view on the problem and on the legislation we've drafted and the challenges we face. We look forward to their testimony.

The Cybersecurity Act of 2012 does several important things to beef up our defenses in the new battleground of cyberspace.

First, it ensures that the cyber systems that control our most critical, privately-owned and operated infrastructure are secure. That's the key here—privately owned and operated cyber infrastructure can well be and probably someday will be the target of an enemy attack. Today it is the target of economic exploitation and we've got to work with the private sector to better secure those systems, both for their own defense and for our national defense.

In this bill, the systems that will be asked to meet standards are defined as those that if brought down or commandeered would lead to mass casualties, evacuations of major population centers, the collapse of financial markets, or significant degradation of security. So this is a tight and high standard. After identifying the systems that meet those standards, under the legislation, the Secretary of Homeland Security would then work with the private sector operators of the systems to develop security performance requirements.

Owners of the privately owned cyber systems covered would have the flexibility to meet the performance requirements with whatever hardware or software they choose, so long as it achieves the required level of security. The Department of Homeland Security will not be picking technological winners or losers and there's nothing in the bill that would stifle innovation. In fact, a letter from Cisco Systems and Oracle, two of our most prominent IT companies concludes that this legislation "includes a number of tools that will enhance the nation's cybersecurity without interfering with the innovation and development processes of the American IT industry."

Under our legislation, if a company can show the Department of Homeland Security that it already has high cybersecurity standards then it will be exempt from further requirements under this law. Failure to meet the standards will result in penalties that will be determined by the Department during the rulemaking and comment process.

It also creates a streamlined and efficient cyber organization within DHS that will work with existing federal regulators and the private sector to ensure that no rules or regulations are put in place that either duplicate or are in conflict with existing requirements.

The bill also establishes mechanisms for information sharing between the private sector and the federal government and among the private sector operators themselves. This is important because computer security experts need to be able to compare notes to protect us from this threat. But the bill also creates security measures and oversight to protect privacy and preserve civil liberties. Privacy and civil liberties advocates have indicated

that our bill provides some of the best privacy and civil liberties protections of the various proposals being discussed in Congress.

The process by which we reached this cybersecurity legislation was very inclusive. We not only worked across committee lines, but reached out to people in business, academic, civil liberties and privacy, and security experts for advice on many of the difficult issues any meaningful piece of cyber legislation would need to address. I can tell you that literally hundreds of changes have been made to this bill as a result of this input and we think we've finally struck the right balance.

I briefly want to mention some things that are not in this bill. First and foremost, this bill does not contain a "kill switch" that would allow the President to seize or control part of or the entire internet in a national crisis. It's not there. It never was. But we put an exclamation point by dropping a section people thought included a "kill switch." It just wasn't worth it because of the urgent need for this bill.

There is nothing in this bill that touches on the balance between intellectual property and free speech that so aroused public opinion over the proposed "Stop Online Privacy Act," or the "Protect IP Act" and left many of my colleagues with scars or post-traumatic stress syndrome. In fact, this is not the ultimate verification of my assertion that there's nothing like what concerned people with SOPA or PIPA, but I note with gratitude one of our witnesses, Mr. Stewart Baker, was a leading opponent of SOPA, but is testifying today in favor of our bill.

After the Cybersecurity Act of 2012 becomes law, the average internet user will go about using the internet just as they do today. But hopefully as a result of the law and outreach they'll be better equipped to protect their own privacy and resources from cyber attack.

The bottom line is a lot of people have worked very hard and in a very bipartisan way to face a real and present danger to our country that we simply cannot allow this moment to slip away from us. I feel very strongly that we need to act now to protect America's cyberspace as a matter of national and economic security.

Statement of Ranking Member
Senator Susan M. Collins
"Securing America's Future: The Cybersecurity Act of 2012"
Thursday, February 16, 2012

After the 9/11 attacks, we learned of many early warnings that went unheeded, including an FBI agent who warned that one day people would die because of the "wall" that kept law enforcement and intelligence agencies apart. When a major cyber attack occurs, the ignored warnings will be even more glaring – because our nation's vulnerability has already been demonstrated by the daily attempts by nation-states, terrorists groups, cyber criminals, and hackers to penetrate our systems.

The warnings of our vulnerability to a major cyber attack come from all directions and countless experts, and are underscored by the intrusions that have already occurred. Earlier this month, FBI Director Robert Mueller warned that the cyber threat will soon equal or surpass the threat from terrorism. He argued that we should be addressing the cyber threat with the same intensity we have applied to the terrorist threat.

Director of National Intelligence James Clapper made the point even more strongly, describing the cyber threat as a "profound threat to this country, to its future, its economy and its very being."

Last November, the director of the Defense Advanced Research Projects Agency or DARPA warned that malicious cyber attacks threaten a growing number of the systems we interact with daily – like the power grid, water treatment plants, and key financial systems.

Similarly, General Keith Alexander, commander of U.S. Cyber Command and director of the National Security Agency, warned that the cyber vulnerabilities we face are extraordinary and characterized by "a disturbing trend, from exploitation to disruption to destruction."

These statements are just the latest in a chorus of warnings from current and former officials. The threat is not just to our national security, but also to our economic well-being. A Norton study last year calculated the cost of global cybercrime at 114 billion dollars annually. When combined with the value of time victims lost due to cybercrime, this figure grows to 388 billion dollars globally, which Norton described as "significantly more" than the global black market in marijuana, cocaine and heroin combined.

In an op-ed last month titled, "China's Cyber Thievery Is National Policy— And Must Be Challenged," former DNI Mike McConnell, former Homeland Security Secretary Michael Chertoff and former Deputy Secretary of Defense William Lynn, noted the ability of cyber terrorists to "cripple" our critical infrastructure, and they sounded an even more urgent alarm about the threat of economic cyber espionage.

Citing an October 2011 report by the Office of the National Counterintelligence Executive, these experts warned of the catastrophic impact that cyber espionage - particularly espionage pursued by China - could have on our economy and competitiveness. They estimated that the cost "easily means billions of dollars and millions of jobs."

This threat is all the more menacing because it is being pursued by a global competitor seeking to steal the research and development of American firms to undermine our economic leadership. As the 2011 report by the U.S.-China Economic and Security Review Commission made clear, China continues to conduct a range of malicious cyber activities "to facilitate industrial espionage and the compromise of U.S. and foreign government computer systems."

The evidence of our cybersecurity vulnerability is overwhelming and compels us to act now. Some members have called for yet more hearings, studies, and mark-ups. In other words, more delay. The fact is, since 2005, our Committee alone has held 10 hearings on the cyber threat, including today's hearing. In 2010, Chairman Lieberman, Senator Carper, and I introduced our cyber security bill, which was reported by this Committee later the same year. Since last year, we have been working with Chairman Rockefeller to merge our bill with legislation he has championed, which was reported by the Commerce Committee. After incorporating changes based on the feedback from the private sector, our colleagues, and the Administration, we have produced a refined version, which is the subject of today's hearing. Chairman Rockefeller and Chairman Feinstein have also devoted countless months working on this vital issue. It is significant that three Senate chairmen with jurisdiction over cybersecurity have come to agreement on these issues. And each day we fail to act, the threat increases to our national and economic security.

Some of our colleagues have urged us to focus narrowly on the Federal Information Security Management Act, as well as on federal research and development and improved information sharing. We *do* need to address these issues - and our bill *does*.

However, with 85 percent of our nation's critical infrastructure owned by the private sector, the government also has a critical role in ensuring that the most vital parts of our infrastructure - those whose disruption could result in truly catastrophic consequences - meet reasonable, risk-based performance standards.

In an editorial this week, the *Washington Post* concurred, writing that our "critical systems have remained unprotected. To accept the status quo would be an unacceptable risk to U.S. national security."

Some of our colleagues are skeptical about the need for any new regulations. I have opposed efforts to expand regulations that would burden our economy. But regulations that are necessary for our national security and that promote - rather than hinder - our economic prosperity strengthen our country.

This bill reflects the extensive consultations we have had while still achieving the goal of improving the security of critical cyber systems. I look forward to discussing the bill with our witnesses today, and I thank the Chairman for calling this hearing and for the leadership he has shown on this vitally important issue.

FOR IMMEDIATE RELEASE: February 16, 2012
Contact: Jesse Broder Van Dyke 202-224-7045
jesse_brodervandyke@akaka.senate.gov

STATEMENT OF SENATOR DANIEL K. AKAKA

Securing America's Future: The Cybersecurity Act of 2012

Hearing
Senate Committee on Homeland Security and Governmental Affairs

Thank you, Mr. Chairman, for holding this hearing. I applaud your tenacity, and that of Ranking Member Susan Collins, Commerce Committee Chairman Jay Rockefeller, and Intelligence Committee Chairman Dianne Feinstein in pursuing the comprehensive cybersecurity legislation we are considering today. I also want to thank you and the Administration for incorporating my suggestions to the cyber workforce provisions of the bill. Employees of the Department of Homeland Security are on the front lines of countering the cyber threat, and we must make sure the Department has the appropriate tools to attract and retain the workforce it needs to meet these complex challenges.

Stakeholders have raised concerns about the privacy and civil liberties implications of certain provisions of this bill. I want to commend the bill's authors for making progress in addressing these concerns. It is important for the final product to adequately protect Americans' reasonable expectation of privacy, and I will continue to closely monitor this issue.

Federal Bureau of Intelligence Director Robert Mueller's recent statement that the danger of cyberattacks will equal or surpass the danger of terrorism in the foreseeable future is a stark reminder that strengthening cybersecurity must be a key priority for this Congress. Cyber criminals and terrorists are targeting our critical infrastructure, including our electricity grids, financial markets, and transportation networks. American businesses face constant cyber attacks that seek to steal their intellectual property and trade secrets. However, cybersecurity policy has been slow to adjust to these ever increasing and sophisticated cyber threats.

The Cybersecurity Act of 2012 will give the Federal government and the private sector the tools necessary to respond to these troubling threats. Finalizing this important legislation is a pressing priority for this Congress, and I look forward to continuing to work with you on it.

FOR RELEASE: February 16, 2012
CONTACT: Emily Spain, (202) 224-2441 or emily_spain@carper.senate.gov

U.S. SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING: "Securing America's Future: The Cybersecurity Act of 2012"

WASHINGTON – Today, Sen. Tom Carper (D-Del.), Member of the Senate Committee on Homeland Security and Governmental Affairs and Chairman of the Subcommittee on Federal Financial Management, Government Information, Federal Services, and International Security, participated in the hearing, "Securing America's Future: The Cybersecurity Act of 2012."

A copy of his opening statement, as prepared for delivery, follows:

I would like to thank Chairman Lieberman and Ranking Member Collins for calling this hearing and for working with me on this very important piece of legislation that we are discussing today.

Nearly every week, we learn of a new cyber attack on our critical infrastructure, government systems, and businesses, and it appears that there is little relief in sight. According to FBI Director, Robert Muller, cyber threats will equal or surpass the threat of terrorism in the foreseeable future. While some hackers want to just cause mischief or make a political point, others want to hurt people. Still others want to steal our ideas, the ingenuity that supports the technologies and breakthroughs that fuel our economy and make us a great country. In order to protect lives and our trade and technological competitiveness, we must put a stop to these threats.

With the introduction of the Cybersecurity Act of 2012, the Senate has once again taken a bold step to protect information systems in our country and better secure the critical infrastructure that we rely on every day for water, energy, and transportation among other daily needs. Our critical infrastructure is what keeps this great nation running, and we must do everything we can to protect these prime targets. The legislation that we will be discussing today would strengthen the electronic backbone of our most sensitive critical infrastructure by creating stronger cyber security standards for the sectors that are most vulnerable. Of course, the federal government cannot do this alone and that is why we are looking to build a true partnership between the key agencies and the private sector so that we can share information more freely.

I am particularly pleased that the legislation includes a number of security measures that I have worked on for years to better protect our federal information systems. The public expects that agencies holding our medical records, Social Security numbers, proprietary business information, and military secrets will take every precaution necessary to ensure that it is secure

and well-protected. This bill will help do that by replacing our outdated, paper-based security practices with a real-time security system that can help our government fight the rapidly evolving and highly agile cyber threats we face today.

The bill also includes several workforce and research initiatives that I have been pushing to help develop the next generation of American cyber professionals. It makes an important investment in education, for example, by providing stronger cybersecurity training and establishing better cybersecurity programs in our schools and universities. Research and development for cyber security is also enhanced in the bill, a provision that can lead to the development of cutting edge technologies here at home that can help us stay one step ahead of our adversaries.

I look forward to hearing from our distinguished panel of witness about the bill and also to working with my colleagues to bring it to the floor. I recognize that there are many good ideas out there about how we can make our country safer from cyber attacks, but we can no longer afford to sit by and wait while hackers, criminal organizations, and countries attack us, putting our economic competitiveness and even our lives at risk with the click of a mouse. The time to act is now.

SENATOR JOHN MCCAIN
OPENING STATEMENT
COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
HEARING: CYBERSECURITY ACT of 2012
FEBRUARY 16, 2012

Mr. Chairman and Ranking Member, thank you for holding this hearing on the long awaited 'Cybersecurity Act of 2012.' I welcome our panel, and specifically, Senators Rockefeller and Feinstein, Secretary Napolitano, and Governor Ridge and thank everyone for the willingness to share their perspective.

I would like to state from the outset that I have sincere fondness and respect for the Chairman and Ranking Member – especially when it comes to matters of national security. So, whatever criticisms I may have with the legislation, should not be interpreted as an attack on the lead sponsors, but rather on the process by which the bill is being debated and it's policy implications.

All of us recognize the importance of cybersecurity in the digital world. Time and again, we have heard from experts about the importance of possessing the ability to effectively prevent and respond to cyber threats. We have listened to accounts of cyber espionage originating in countries like China; organized cyber criminals in Russia; and rogue outfits with a domestic presence like 'Anonymous,' who unleash cyber-attacks on those who dare to politically disagree. Our own Government Accountablity Office has reported that over the last five years, cyber-attacks against the United States are up 650 percent. The threat is real.

It is my opinion that Congress should be able to address this issue with legislation a clear majority of us can support. However, we should begin with a transparent process which allows lawmakers, and the American public to let their views be known. Unfortunately, the bill introduced by the Chairman and Ranking Member has already been placed on the calendar by the Majority Leader, without a

single markup or any executive business meeting by any committee of relevant jurisdiction. My friends, this is wrong.

To suggest that this bill should move directly to the Senate Floor because it has "been around" since 2009 is outrageous. First, the bill was introduced two days ago. Secondly, where do Senate Rules state that a bill's progress in a previous congress can supplant the necessary work on that bill in the present one? Additionally, in 2009 we were in the 111th Congress with a different set of Senators. For example, the minority of this Committee has four Senators who were not even in the Senate, much less on this Committee, in 2009. How can we seriously call it a HSGAC product without their participation in committee executive business? Respectfully, to treat the last Congress as a legislative mulligan by bypassing the committee process and bringing the legislation directly to the floor is not the appropriate way to begin consideration of an issue as complicated as cybersecurity.

In addition to these valid process concerns, I also have policy issues with the bill.

A few months ago, the Chairman of this Committee and I introduced an amendment to the Defense Authorization bill codifying an existing cybersecurity Memorandum of Agreement (MOA) between the Department of Defense and the Department of Homeland Security (DHS). The purpose of that amendment was to ensure that this relationship endures and highlight that the best government-wide cybersecurity approach is one where DHS leverages, not duplicates DoD efforts and expertise. This bill, unfortunately, backtracks on the principles of the MOA, by expanding the size, scope, and reach of DHS and neglects to afford the authorities necessary to protect the homeland to the only institutions currently capable of doing so, U.S. Cybercommand and the National Security Agency (NSA).

At a recent FBI-sponsored symposium at Fordham University, General Keith Alexander, the Commander of U.S. Cybercommand and the Director of the NSA stated that if a significant cyber attack against this country were to take place there may not be much that he and his teams at either Cybercommand or NSA can legally do to stop it in advance. According to General Alexander, "in order to stop a cyber attack you have to see it in real time, and you have to have those authorities. Those are the conditions we've put on the table...Now how and what the Congress chooses, that'll be a policy decision." This legislation does nothing to address this significant concern and I question why we have yet to have a serious discussion about who is best suited to protect our Country from this threat we all agree is very real and growing.

Additionally, if the legislation before us today were enacted into law, unelected bureaucrats at the DHS could promulgate prescriptive regulations on American businesses – which own roughly 90 percent of critical cyber infrastructure. The regulations that would be created under this new authority would stymie job-creation, blur the definition of private property rights and divert resources from actual cybersecurity to compliance with government mandates. A super-regulator, like DHS under this bill, would impact free market forces which currently allow our brightest minds to develop the most effective network security solutions.

I am also concerned about the cost of this bill to the American taxpayer. The bill before us fails to include any authorizations or attempt to pay for the real costs associated with the creation of the new regulatory leviathan at DHS. This attempt to hide the cost is eclipsed by the reality that the assessment of critical infrastructure, the promulgation of regulations and their enforcement will take a small army.

Finally, I'd like to find out over the next few days what specific factors went into providing regulatory carve-outs for the IT hardware and software manufacturers? My suspicion is that this had more to do with garnering political support and legislative bullying than sound policy considerations. However, I think the fact that such carve outs are included only lends credence to the notion that we shouldn't be taking the regulatory approach in the first place.

Because of provisions like these and the threat of a hurried process, myself, and Senators Hutchison, Chambliss, Murkowski, Grassley and others are left with no choice but to introduce an alternative cybersecurity bill in the coming days. The fundamental difference in our alternative approach is that we aim to enter into a cooperative relationship with the entire private sector through information sharing, rather than an adversarial one with prescriptive regulations. Our bill, which will be introduced when we return from the President's Day recess, will provide a common-sense path forward to improve our nation's cybersecurity defenses. We believe that by improving information sharing among the private sector and government; updating our criminal code to reflect the threat cyber criminals pose; reforming the Federal Information Security Management Act; and focusing federal investments in cybersecurity; our nation will be better able to defend itself against cyber attacks. After all, we are all partners in this fight, and as we search for solutions, our first goal should be to move forward together.

United States Senate

WASHINGTON, DC 20510

February 14, 2012

Senator Harry Reid
Senate Majority Leader
United States Senate
Washington, D.C. 20510

Senator Mitch McConnell
Senate Minority Leader
United States Senate
Washington, D.C. 20510

Dear Leaders Reid and McConnell:

As the President was informed in a November letter, we share the concern that our nation may be vulnerable to cyberthreats, and we recognize the need to take appropriate steps to secure our infrastructure from attack. However, we have yet to find broad bipartisan agreement on the most effective legislative solution.

This very important and complex issue covers a significant part of our infrastructure and our economy. Not only are our government agencies and defense contractors implicated for national security purposes, but state and local governments and a broad cross-section of industries (including transportation, energy, Internet technology, telecommunications, healthcare, agriculture and financial industries) will likely be covered under the umbrella of "cybersecurity." Consequently, this issue involves the jurisdiction of multiple committees, especially those upon which we serve as Ranking Members—Commerce, Intelligence, Judiciary, Energy, Armed Services, Budget and Health, Education, Labor and Pensions.

Each of us recognized from the earliest consideration of cybersecurity legislation that addressing the threat would necessarily involve issues that crossed committee jurisdictions and some wanted the committee processes to play out. Senator John McCain, the Ranking Member of the Armed Services Committee, appreciated this challenge and recommended the creation of a Select Committee. Instead the Majority leader established bipartisan working groups to consider substantive aspects of cybersecurity legislation across committee responsibilities. Unfortunately, the working groups met infrequently—if at all—and did not function constructively.

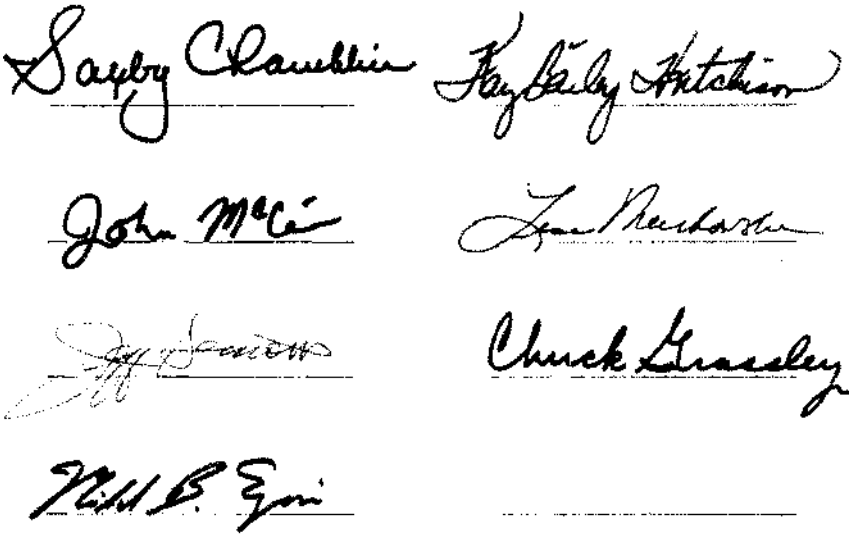
The Chair and Ranking Member of the Committee on Homeland Security and Government Affairs have recently introduced their latest legislative proposal, which as drafted, does not satisfy our substantive concerns, nor does it satisfy our process concerns. Given the serious national security and economic consequences of any legislation, it is imperative that the other committees of jurisdiction be given the opportunity to shape the legislative outcome in a

bipartisan manner. If we are serious about enacting effective legislation into law, we must provide all Members of the Senate the opportunity to become adequately informed by regular order. This is not the kind of legislation that can result in a carefully balanced solution unless the full process is afforded.

While some committees have held hearings and executive business meetings on other cyber-related bills within their jurisdiction, the relevant committees have not had the opportunity to weigh in on this measure even though it cuts across committee jurisdictions. We call upon our Senate Leadership to allow the committees of jurisdiction to convene hearings and conduct executive business meetings on this new bill so that Senators can be properly educated on this complicated measure and the committees of jurisdiction can provide their necessary perspective before any measure is brought to the Senate floor for consideration. This process is in keeping with the Majority Leader's commitment to provide "Senators, the Administration, and non-governmental stakeholders an opportunity to review the legislation prior to floor consideration, and to an open floor debate."

We look forward to working with you on this important issue.

Sincerely,



Statement of Senator John D. Rockefeller IV

Senate Committee on Homeland Security and Governmental Affairs
Hearing on the Cybersecurity Act of 2012
February 16, 2012

Chairman Lieberman, Senator Collins, and distinguished Members of the Committee on Homeland Security and Governmental Affairs, I am honored to be here today to urge the Senate to move on the Cybersecurity Act of 2012.

It's an important bill, and I will fight for its passage. I look forward to the time when Secretary Napolitano and the Department of Homeland Security, which has made such important strides in this area, can begin implementing the protections that this bill provides for.

Our government needs a lead **civilian** agency to coordinate our civilian cybersecurity efforts, and that agency should be the one that has that responsibility now: The Department of Homeland Security.

I want to emphasize that our bill represents the expertise and hard work of three Senate Committees, and the input of many other Senators and outside stakeholders, over the course of the past three years.

We have eagerly sought – and have received – constructive criticism and input from all corners. Anyone and everyone who wanted to protect our country from the cyber threat had a seat at the table.

Even when people refused to engage with us, we tried to find their ideas and put them in the bill. A couple of weeks ago we took ideas from an op-ed that fellow Senators wrote.

Beyond this bill's principal authors – Senators Lieberman, Collins, Feinstein and I – this bill reflects the input, assistance, or requests of Senators on both sides of the aisle.

Senator Snowe was my co-author of the bill that Commerce reported out last year. Senator Carper was a co-author of the Lieberman-Collins bill. Both have left a major imprint on this bill, and I consider them partners in moving this ahead.

Senator Hutchison and her staff worked with us for a good part of the past two years, and we have tried hard to address all of her specific concerns. I think we have done so in virtually every case.

We have sought to engage Senator Chambliss, and before him, Senator Bond, in the same fashion.

Senators Kyl and Whitehouse contributed an entire title regarding cyber public awareness, and Senators Kerry, Lugar, Gillibrand and Hatch did the same on the title regarding diplomacy.

Because of Senator McCain's concerns, we omitted significant language pertaining to the White House cyber office.

And when colleagues had ongoing questions about a provision that I personally believe is extremely important, I agreed to drop it from the base bill. This provision would clarify private sector companies' **existing** requirements regarding what "material risks" pertaining to cyber have to be disclosed to investors in SEC filings.

I believe this provision is absolutely crucial for the market to help solve our cyber vulnerabilities and will fight for it as an amendment on the floor. But in the interest of providing more time to address colleagues' questions, I agreed to take it out of the bill that we introduced this week.

Any suggestion that this exhaustive process has been anything but open and transparent is **simply false**.

Why have we worked so tirelessly to include the views of all sides? Why have we tried so hard to get this right?

Because our country and our communities and our citizens are at grave risk. This is not a Republican or Democrat issue, it's a life or death issue.

I want to be clear: The cyber threat is a very real fact. This is not alarmism. Here's why:

Hackers supported by the governments of China and Russia, and also sophisticated criminal syndicates with potential connections to terrorist groups, are now able to crack the codes of our government agencies, our Fortune 500 companies and everything in between.

They are looting our country of our most valuable possessions on an unfathomable scale. But that's not the end of the problem.

The reason that this cyber **theft** is a life or death issue is the same as the reason that a burglar in your house is a life or death issue. If a criminal has broken into your home, how do you know all he wants to do is steal your belongings?

How do you know he's not going to hurt you or your family?

That's the situation we face right now. Cyber burglars have broken in, and they have destructive cyber weapons that could do us great harm.

That's why Admiral Mike Mullen, former Joint Chiefs Chairman, said that the cyber threat is the only other threat that's on the same level as Russia's stockpile of nuclear weapons.

And FBI Director Robert Mueller testified to Congress recently that the cyber threat will soon overcome terrorism as the **top** national security focus of the FBI.

Think about that – cyber threats will be as dangerous as terrorism. Cyber threats could be as devastating to this country as the terror strikes that tore apart this country just 10 years ago.

Think about how many people could die if a cyber terrorist attacked our air traffic control system and planes slammed into one another.

Or if rail switching networks were hacked - causing trains carrying people – or hazardous materials – to derail or collide in the midst of some of our most populated urban areas, like Chicago, New York, San Francisco or Washington.

We're on the brink of what could be a calamity on any given day – at a time that is not our choosing. That's why the Directors of National Intelligence under both President George W. Bush and President Barack Obama have said that the cyber threat is the number one threat to our country.

We can act now, and try and prepare ourselves. Or we can wait and face the consequences.

I'm here to argue that we should act now to prevent a cyber disaster.

That's what our bill would do.

It's premised on companies taking responsibility for securing their own networks, with government assistance where necessary. It focuses like a laser on protecting the most critical networks, and it promotes the innovation of the private sector market for information technology products and services.

This bill is a good product that has had its tires kicked for three years. It has already garnered significant praise from key industry groups and civil liberties advocates. I am very proud of what we have done.

We have a solemn responsibility to act before it's too late.

Ten years ago, throughout 2001, our national security systems warned us about the possibility of a terrorist threat. We know now that we failed to take sufficient action to address those threats. And we paid for it.

I think back to 2000 and 2001, when we saw signs of people moving in and out of our country, we saw dots appear to connect, and we knew something new and different and dangerous might be upon us.

Our intelligence and national security leadership took these matters seriously – but not seriously enough.

Then it was too late. 9/11 happened.

Today, with a new set of warnings flashing before us, and a wide range of new challenges to our security and our safety, we again face a choice.

Act now, and put in place safeguards to protect this country and our people. Or act later, when it is too late. I urge the Senate to act now.

Testimony of Senator Feinstein
Homeland Security & Governmental Affairs Committee
"Cybersecurity Act of 2012"
Thursday, February 16, 2012, 2:30 pm

Chairman Lieberman and Ranking Member Collins, thank you for holding this hearing. I want to thank both of you – as well as Chairman Rockefeller – for your leadership on this issue and your major efforts over the past two Congresses on cybersecurity.

I am pleased to join the three of you as an original co-sponsor of the "**Cybersecurity Act of 2012**," which is a comprehensive bill to improve the cybersecurity of both the private sector and the federal government.

The Growing Problem of Cyber Intrusions:

Like you, the Intelligence Committee has examined the cyber threats to our national and economic security. Just last month, at our worldwide threats hearing, the U.S. Intelligence Community's official written testimony equated cyber threats to terrorism and proliferation as the highest priority threats to our security.

FBI Director Robert Mueller testified that "***the cyber threat, which cuts across all programs, will be the number one threat to the country***."

Already, cyber attacks are doing great damage to the United States, and the trend is getting worse. Consider the following four examples, each of which is only the unclassified tip of a much larger iceberg:

- **The Pentagon's networks are being probed thousands of times daily** and its classified military computer networks suffered a "significant compromise" in 2008 according to former Deputy Defense Secretary Bill Lynn.

- In November 2009, DOJ charged 7 defendants from Estonia, Russia, and Moldova with hacking into the **Royal Bank of Scotland and stealing $9 million** from more than 2,100 ATMs in 280 cities worldwide in 12 hours.

- In 2009, Federal officials indicted 3 men for **stealing data from more than 130 million credit cards by hacking into 5 major companies' computer systems**, including 7-Eleven, Heartland Payment Systems, and the Hannaford Brothers supermarket chain.

- Finally, an unclassified report by the Intelligence Community in November 2011 said **cyber intrusions against U.S. companies cost untold billions of dollars annually and named China and Russia as aggressive and persistent cyber thieves**.

Modern warfare is already employing cyber attacks, as seen in Estonia and Georgia. And unfortunately, it may only be a matter of time before we see cyber attacks that can cause catastrophic loss of life, whether by terrorists or state adversaries.

Our enemies are constantly on the offensive and in the cyber domain, it is much harder for us to play defense than it is for them to attack. The key question is: "*What do we do about this dangerous and growing cyber threat?*"

I believe the comprehensive bill that has been introduced – the Cybersecurity Act of 2012 – is an essential part of the answer.

Improving Cyber Information Sharing (Feinstein Bill):

I'd like to speak briefly on the cybersecurity information sharing bill that I introduced on Monday, and that you have included as Title Seven in your legislation.

The goal of this bill is to improve the ability of the private sector and the government to share information on cyber threats that both sides need to improve their defenses.

However, a combination of existing law, the threat of litigation, and standard business practices has prevented or deterred private sector companies from sharing information about the cyber threats they face and the losses of information and money they suffer. We need to change that through better information sharing, in a way that companies will use, that protects privacy interests, and that takes advantage of classified information without putting that information at risk.

What Title VII: "Information Sharing" Does:

Specifically, Title VII of the Cybersecurity Act of 2012:

(1) Affirmatively provides private sector companies the authority to monitor and protect the information on their own computer networks.

(2) Encourages private companies to share information about cyber threats with each other by providing a good faith defense against lawsuits for sharing or using that information to protect themselves.

(3) Requires the Federal government to designate a single focal point for cybersecurity information sharing. We refer to this as a "Cybersecurity Exchange," to serve as a hub for appropriately *distributing* and *exchanging* cyber threat information between the private sector and the government. This is intended to reduce government bureaucracy and make the government a more effective partner of the private sector, but with protections to ensure that private information is not misused. This legislation provides no new authority for government surveillance.

3

(4) Establishes procedures for the government to share classified cybersecurity threat information with private companies that can effectively use and protect that information. This is a prudent way to take advantage of the information that the Intelligence Community acquires, without putting our sources and methods at risk, or turning private cybersecurity over to our intelligence apparatus.

The Need for Data Breach Legislation:

Mr. Chairman, I would like to raise one issue that is not yet included in this cyber-security package: **data breach notification.**

This is an issue I have worked on for over eight years, and it is in urgent need of attention in the Senate. My current bill – the Data Breach Notification Act – has been approved by the Judiciary Committee, and accomplishes what are, in my view, the key goals of any data breach notification legislation:

1. Notice to individuals, who will be better able to protect themselves from identity theft;
2. Notice to law enforcement, which can connect the dots between breaches and cyber-attacks; and
3. Preemption of the 47 different state and territorial standards on this issue, so companies are not subjected to often-conflicting regulation by the states.

I know that Senators Rockefeller and Pryor have a bill on this topic in the Commerce Committee, and that Senators Leahy and Blumenthal have their own bills that were reported out of the Judiciary Committee.

The differences between our approaches are not so great that we cannot work them out, and I am prepared to sit down with members of this Committee, with Senator Rockefeller, and others to find a common solution.

In sum, I look forward to the consideration of this comprehensive cyber legislation and I hope it will be taken up by the Senate soon. Thank you very much for the opportunity to testify on this important issue.

Statement for the Record
Of

Secretary Janet Napolitano
U.S. Department of Homeland Security

Before the
United States Senate
Homeland Security and Governmental Affairs
Committee
Washington, DC

February 16, 2012

Chairman Lieberman, Ranking Member Collins, and Members of the Committee, it is a pleasure to appear before you today to discuss the critical issue of cybersecurity. I appreciate the opportunity to explain the Department of Homeland Security's (DHS) cybersecurity mission and how new legislation will strengthen our ability to protect the Nation. Specifically, I want to express the Department's strong support for the Cybersecurity Act of 2012. The Department of Homeland Security appreciates the leadership of Chairman Lieberman and Ranking Member Collins, as well as Senators Rockefeller and Feinstein, who have worked in a bipartisan manner over many months and years, to address the core national security requirements and economic interests also laid out in the Administration's legislative proposal. The Cybersecurity Act of 2012 would provide the comprehensive tools we need to effectively address the full range of cyber threats facing our nation, while preserving privacy and civil liberties and respecting freedom, openness, and innovation. As the President noted in the State of the Union address, addressing the dangers of cyber threats is critically important for our nation, and quickly enacting this legislation would be an incredibly important step.

The United States confronts a dangerous combination of known and unknown vulnerabilities in the cyber domain, strong and rapidly expanding adversary capabilities, and limited threat and vulnerability awareness. While we are more network dependent than ever before, increased interconnectivity increases the risk of theft, fraud, and abuse. No country, industry, community or individual is immune to cyber risks. Our daily life, economic vitality, and national security depend on cyberspace. A vast array of interdependent IT networks, systems, services, and resources are critical to communication, travel, powering our homes, running our economy, and obtaining government services.

In addition to risks and vulnerabilities, cyber incidents have increased dramatically over the last decade. There have been instances of theft and compromise of sensitive information from both government and private sector networks, undermining confidence in our systems, information sharing processes, and the integrity of the data contained within these systems. Last year, the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

Recognizing the serious nature of this challenge, President Obama made cybersecurity an Administration priority upon taking office. During the release of his Cyberspace Policy Review in 2009, which established a strategic framework for advancing the Nation's cybersecurity policies, the President declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation."

Cybersecurity is a shared responsibility, and each of us has a role to play. Emerging cyber threats require the engagement of our entire society—from government and law enforcement to the private sector and most importantly, members of the public. The key question, then, is how do we address this problem? This is not an easy question, because cybersecurity requires a layered approach. The success of our efforts to reduce cybersecurity risks depends on effective communication and partnerships among departments and agencies from all levels of government, the private sector, international entities, and the American public.

RESPONSIBILITIES AND ACCOMPLISHMENTS

DHS works with federal agencies to secure unclassified federal civilian government networks and works with owners and operators of critical infrastructure to secure their networks through risk assessment, mitigation, and incident response capabilities. To protect Federal civilian agency networks, we are deploying technology to detect and block intrusions in those agencies with support from the Department of Defense. We also work to provide agencies with assistance in the implementation of guidance and standards issued by the National Institute of Standards and Technology (NIST). In addition, DHS is responsible for coordinating the national response to significant cyber incidents, consistent with the National Response Framework, and for creating and maintaining a common operational picture for cyberspace across the government.

With respect to critical infrastructure, DHS and the sector specific agencies work with the private sector to help secure the key systems upon which Americans rely, such as the financial sector, the power grid, water systems, and transportation networks. We do this by sharing actionable cyber threat information with our private sector partners, helping companies to identify vulnerabilities before a cyber incident occurs, and providing forensic and remediation assistance to help response and recovery after we learn of a cyber incident. Last year, the DHS Industrial Control Systems Computer Emergency Response Team (ICS-CERT) conducted 78 assessments of control system entities which helped companies identify security gaps and prioritize mitigations. We also empower owners and operators to help themselves by providing a cyber self-evaluation tool, which was utilized by over 1,000 companies last year, as well as in-person and on-line training sessions.

To combat cyber crime, DHS leverages the skills and resources of the U.S. Secret Service, U.S. Immigration and Customs Enforcement, and U.S. Customs and Border Protection and works in cooperation with Department of Justice, especially the Federal Bureau of Investigation, to investigate and prosecute cyber criminals. In FY 2011 alone, DHS prevented $1.5 billion in potential losses through cyber crime investigations and announced charges against 72 individuals for their alleged participation in an international criminal network dedicated to the sexual abuse of children and the creation and dissemination of graphic images and videos of child sexual abuse throughout the world.

DHS also serves as a focal point for cybersecurity outreach and awareness efforts. Raising the cyber education and awareness of the general public creates a more secure environment in which the personal or financial information of individuals is better protected. As we perform this work, we are mindful that one of our missions is to ensure that privacy, confidentiality, and civil liberties are not diminished by our efforts. The Department has implemented strong privacy and civil rights and civil liberties standards into all its cybersecurity programs and initiatives from the outset. DHS has performed Privacy Impact Assessments of our key cybersecurity programs such as EINSTEIN, which provides intrusion detection capabilities to the civilian federal agencies. DHS also receives regular counsel on cybersecurity activities from the Data Privacy and Integrity Advisory Committee (DPIAC), a body of outside experts who advise the Department on ways to address privacy and civil liberties concerns.

CURRENT AUTHORITIES

Congress has granted DHS certain authorities in the area of cyber security. For example, the Homeland Security Act of 2002 specifically directed DHS to enhance the security of non-federal networks by providing analysis and warnings, crisis management support, and technical assistance to State and local governments and the private sector. As part of its critical infrastructure protection mission, DHS also works with the sector specific agencies to carry out vulnerability and risk assessments, identify priorities for protective support measures, and develop a comprehensive national plan for securing the Nation's cyber and communications infrastructure.

Building upon this statutory footing, successive Administrations have assigned the Department key responsibilities in carrying out national cybersecurity efforts. US-CERT has long been designated to carry out the functions of the Federal information security incident center required under the Federal Information Security Management Act (FISMA) to help agencies prevent and respond to cyber incidents on government networks. In July 2010, he Office of Management and Budget assigned DHS primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to Federal information systems.

Several Executive Orders and Presidential Directives have assigned the Department increasing responsibilities related to cybersecurity:

- Executive Order 12472 designates DHS as the Executive Agent for the National Communications System (NCS), which assists the Executive Branch in coordinating the planning and provision of national security and emergency preparedness communications under all circumstances. The NCS is the focal point for joint industry-government national

security and emergency preparedness communications planning, response and restoration during all conditions of crisis or emergency.

- Under Homeland Security Presidential Directive (HSPD) 7, DHS serves as a focal point for the security of cyberspace to facilitate interaction and collaboration between and among Federal departments and agencies, State and local governments, the private sector, academia, and international organizations. DHS also works with the sector specific agencies, as each critical infrastructure sector possesses its own unique characteristics, operating models and risk environment.
- National Security Presidential Directive 54/HSPD 23 directs DHS to manage and oversee consolidated intrusion detection, incident analysis, and cyber response capabilities to better protect Federal networks. DHS also integrates threat and vulnerability information; provides a consultative structure to coordinate the cybersecurity activities of participating Federal cyber centers and ensures that federal agencies have access to information and intelligence needed to execute their respective cybersecurity missions.
- In accordance with HSPDs 23 and 7, DHS disseminates cyber threat, vulnerability, mitigation, and warning information to improve the security and protection of critical infrastructure networks owned or operated by Federal agencies, State, local, and tribal governments; private industry; academia; and international partners.

As its cybersecurity mission continues to evolve, DHS has increased its funding of key programs to keep pace with emerging threats through innovative technologies and services. From FY 2011 to FY 2012, the Department's cyber budget increased by over $80 million or 22 %. The President's FY 2013 Budget request builds on these efforts by making significant investments to expedite the deployment of intrusion detection and prevention technologies on government computer systems, increase federal network security of large and small agencies, and continue to develop a robust cybersecurity workforce to protect against and respond to national cybersecurity threats and hazards. The $769 million FY 2013 budget request for cybersecurity represents a 74% increase over FY 2012.

PARTNERSHIP WITH THE DEPARTMENT OF DEFENSE

The Department of Defense is a key partner in our cybersecurity mission. In 2010, I signed a Memorandum of Understanding with then-Secretary of Defense Robert Gates to formalize the interaction between DHS and the Department of Defense to protect against threats to our critical civilian and military computer systems and networks. Congress mirrored this division of responsibilities in the Fiscal Year 2012 National Defense Authorization Act. We are currently working with the Defense Industrial Base and the Banking and Finance Sector to exchange actionable information about malicious activity. One important goal of the current legislative proposals is to allow DHS to expand and enhance these efforts with critical infrastructure.

WHY NEW LEGISLATION IS NEEDED NOW

While the Administration has taken significant steps to protect against evolving cyber threats, we must acknowledge that the current threat outpaces our current authorities. DHS must execute its portion of the cybersecurity mission under an amalgam of existing statutory and executive authorities that fail to keep up with the responsibilities with which we are charged. Our cybersecurity efforts have made clear that our Nation cannot improve its ability to defend against cyber threats unless certain laws that govern cybersecurity activities are updated.

Members of both parties in Congress have come to the same conclusion; approximately 30 cyber-related bills have been introduced in the last two Congresses. In addition, Majority Leader Reid and six Senate committee chairs wrote to the President and asked for his input on cybersecurity legislation. The Administration welcomed the opportunity to assist these congressional efforts, and in May 2011 we provided a pragmatic and focused cybersecurity legislative proposal for Congress to consider. We believe these proposals provide important steps in improving the cybersecurity posture of the United States.

Since then, we have had many interactions with this Committee and Congress to provide our perspective. Indeed, in the last two years, Department representatives have testified in 16 committee hearings and provided 161 staff briefings. Given this predicate, we are encouraged that legislation has been unanimously reported from this Committee and from the Commerce Committee. We appreciate that you are holding today's hearing as a public forum to discuss these well-developed legislative issues and applaud the Senate leadership's initiative to take your bill to the Senate floor.

I am pleased to see that recently introduced legislation contains great commonality with the Administration's proposal. Enactment of a bill along these common lines will be a major step forward for the Nation's cybersecurity. Indeed, all sides agree that federal and private networks must be better protected, and information about cybersecurity threats should be shared more easily while ensuring that privacy and civil liberties are protected through a customized framework of information handling policies and oversight. Both the Administration's proposal and the Senate legislation would improve operations in those areas by providing DHS with clear statutory authority commensurate with our cybersecurity responsibilities. For example, the important updates to FISMA in both the Administration's proposal and yours will enhance the Executive branch's efforts to transform federal network security efforts from costly and ineffective paperwork exercises to implementation of actual security measures.

In addition, many would agree with the House Republican Cyber Task Force when it said, "Congress should consider carefully targeted directives for limited regulation of particular critical infrastructures to advance the protection of cybersecurity." Both the Administration's

proposal and the Senate legislation recognize the severity and urgency to secure critical infrastructure and take some basic steps in this area.

Accordingly, the Administration proposed risk mitigation guidance to ensure that companies providing the Nation's most essential services are instituting a baseline level of cybersecurity. This proposal would leverage the expertise of the private sector requiring the Nation's most critical infrastructure adopt the cybersecurity practices, technologies, and performance standards that work best on their networks.

There is also broad support for increasing the penalties for cyber crimes and for creating a uniform data breach reporting regime to protect consumers. The Administration's proposal will help protect the American people by enhancing our ability to prosecute cyber criminals and by establishing national standards requiring businesses that have suffered an intrusion to notify affected individuals if the intruder had access to the consumers' personal information.

I believe we have made great progress toward reaching a consensus that will help protect the American people, Federal government networks and systems, and our Nation's critical infrastructure. I hope that the current legislative debate maintains the bipartisan tenor it has benefitted from so far, and builds from the consensus that spans two Administrations and the Committee's efforts of the last several years.

CONCLUSION

In an election year there is a tendency to put off needed legislation. The threats to our cybersecurity are real, they are serious, and they require urgent action. The current legislation before the Senate has bi-partisan support. Numerous current and former homeland and national security officials have expressed their desire to see it passed this year. The time to act is now: to improve cybersecurity coordination, strengthen our cybersecurity posture, and protect all elements of our economy against this serious and growing threat, while protecting privacy, confidentiality, and civil liberties. We look forward to engaging with Congress in the days ahead to reach agreement on a bill that will move the Nation forward.

The Honorable Tom Ridge
Chairman, National Security Task Force, U.S. Chamber of Commerce
U.S. Senate Committee on Homeland Security and Governmental Affairs Committee
Hearing Entitled, "Securing America's Future: The Cybersecurity Act of 2012"
Thursday, February 16, 2012

Good afternoon, Chairman Lieberman, Ranking Member Collins, and other distinguished members of the Homeland Security and Governmental Affairs Committee.

I am Tom Ridge, President and CEO of Ridge Global. Prior to heading Ridge Global, and following the tragic events of September 11th, I became the first Assistant to the President for Homeland Security. In 2003, I was honored to become the first Secretary of the Department of Homeland Security (DHS).

During my tenure, I had the privilege to work with more than 180,000-plus employees from a combined 22 agencies to create an agency that facilitated the flow of people and goods; instituted layered security at air, land, and seaports; developed a unified national response and recovery plan; protected critical infrastructure; integrated new technology; and improved information-sharing worldwide. Before September 11th, I was twice elected Governor of Pennsylvania and served from 1995 to 2001. Prior to being governor, I proudly served in the House of Representatives, beginning in 1982.

I am testifying today on behalf of the U.S. Chamber of Commerce, the world's largest business federation representing the interests of more than 3 million businesses and organizations of every size, sector, and region.

I chair the Chamber's National Security Task Force, which is responsible for the development and implementation of the Chamber's homeland and national security policies. It is composed of 150 Chamber members who represent a broad spectrum of the nation's economy. The Task Force seeks to identify current and emerging issues, craft policies and positions on issues, and provide issue analysis and direct advocacy to government and business leaders.

On behalf of the Chamber and its members, thank you for the opportunity to appear here regarding cybersecurity and ways in which we can secure America's future. I have valued the discussions that we have had on policy when I was in the public sector.

Introduction: Cyberspace Offers Tremendous Opportunities and Challenges

The business community recognizes the opportunities and challenges inherent in our interconnected world. The Internet has transformed the global economy and connected people in new and exciting ways. It helps drive progress in almost every aspect of our lives. Businesses of all sizes are increasingly dependent on the Internet for their day-to-day operations. Cyber technologies help businesses achieve great efficiencies, and they help run our vital infrastructures—from the shop floor to energy production to banking and much more.

Unfortunately, bad actors—such as organized criminals, "hactivists," and foreign governments—have taken advantage of a cyber environment that is more open and welcoming than secure. The Chamber and members of its National Security Task Force are keenly aware of cyber threats to American businesses and the nation. The Director of National Intelligence, James Clapper, recently testified about the scope and nature of cybersecurity incidents as well as the range of actors and targets. His insights help inform our discussion.

An essential question facing policymakers is: How do we continue to develop public policies that improve economic and national security? The Chamber believes there is a growing consensus about measures that can help counter illicit cyber intruders and earn broad bipartisan support, which I will touch on further in my remarks. Over the past few years, the Chamber has stated that it will support legislation, such as an information-sharing bill, that is carefully targeted toward effectively addressing the complex cyber threats that businesses are experiencing.

The Private Sector Strives to Proactively Enhance Its Security and Resilience

Businesses strive to stay a step ahead of cybercriminals and protect potentially sensitive consumer and business information by employing sound risk-management principles. Industry has been taking robust and proactive steps for many years to protect and make their information networks more resilient.

The protection of U.S. critical infrastructure has a lengthy history. Issued in 1998, Presidential Decision Directive No. 63 (PDD-63) helped spur the protection of critical infrastructure and cybersecurity and as well helped launch the formation of Information Sharing and Analysis Centers (ISACs) across the private sector. In 2003, Homeland Security Presidential Directive No. 7 (HSPD-7) updated the policy of the United States and the roles and responsibilities of various agencies related to critical infrastructure identification, prioritization, and protection.

Jumping forward a few years, 2006 witnessed the creation of the National Infrastructure Protection Plan (NIPP) and the Critical Infrastructure Protection Advisory (CIPAC). The NIPP resulted in the establishment of Sector Coordinating Councils and Government Coordinating Councils to work together on furthering the protection and resilience of the critical infrastructure community under the authorities of CIPAC. The NIPP was revised in 2009 to reflect an evolution of the process, including expanded integration of all-hazard and similarly important principles.

Businesses are heavily focused on guarding their operations from interruption, preventing the loss of capital or intellectual property, and protecting public safety. They devote considerable resources toward maintaining their operations in the wake of a natural hazard or man-made threat, such as a cyberattack. Business owners and operators understand it is imperative that information infrastructure be well protected and resilient.

Cybersecurity is viewed as an essential aspect of risk reduction, just like risk management related to physical threats. Industry activities have included development of guides, road maps, and standards to improve security, operational safety, and reliability. Sector leaders undertake exercises, which the Chamber encourages, to assess and improve facility and system

capabilities. In sum, private-sector owners and operators routinely strive to strengthen the security of their cyber systems and identify and mitigate any network vulnerability.

The businesses community already complies with multiple information security rules. Among the regulatory requirements impacting businesses of all sizes are the Chemical Facilities Anti-Terrorism Standards (CFATS), the Federal Energy Regulatory Commission-North American Reliability Corporation Critical Information Protection (FERC-NERC CIP) standards, the Gramm-Leach-Bliley Act (GLBA), the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes-Oxley (SOX) Act. Instead of adding to the regulatory burden, Congress should work to reduce the fragmented and often conflicting burdens that these different rules and bureaucracies place on industry.

More Regulation Would Impede Partnerships, Cybersecurity, and Innovation

The Cybersecurity Act of 2012 would authorize DHS to establish a regime for regulating the assets or systems of vital parts of the American economy. Given the discretion that government officials would have in designating "covered" critical infrastructure (CCI), the likelihood for DHS to regulate entities in many American communities is considerable. Instead of taking this less optimal route, the Chamber believes that policymakers should utilize and improve upon the sector-based risk assessments already being conducted by DHS.

Advocates of a regulatory CCI program argue, "We propose a 'light-touch' approach to regulation." However, the Chamber is concerned not only with the concept but with how it would be implemented. During the implementation phase of a regulatory CCI program, it would likely shift from being standards- and risk-based and flexible in concept to being overly prescriptive in practice.

A regulatory program would likely become highly rigid in practice and thus counterproductive to effective cybersecurity—due in large part to a shift in businesses' focus from security to compliance. Equally concerning, federal mandates could compromise security. By homogenizing security, our online adversaries would quickly learn to circumvent a company's protections and those of similarly situated companies.

It is not unreasonable to think that Congress, with the myriad issues on its plate, would find it challenging to maintain a level of vigilance necessary to ensure that the regulatory CCI program does not become prescriptive and detrimental to security. Contrary to some news headlines, the private sector routinely thwarts cyberattacks against its networks because it is fast and nimble in its response and recovery efforts. The Chamber is deeply concerned that a new regulatory regime would box in our critical infrastructures, hampering the freedom, agility, and innovation needed to deflect or defeat adversaries who are often quite amply resourced.

In addition to a regulatory CCI program, the Chamber is concerned about proposals that call on the owners and operators of CCI to develop risk mitigation plans that would be evaluated by a third-party auditor. Complying with third-party assessments would be costly and time consuming, particularly for small businesses. Most businesses already have processes in place for assessing and improving the strength of their networks, so added mandates are unnecessary if

not misguided. Many in the business community are concerned that the release of proprietary information to third parties could actually create new security risks.

Also, the Chamber opposes any proposal requiring CCI to report any significant cyber incident to DHS or another government body. Information sharing is a two-way street, but this incredibly broad reporting threshold would be unworkable in practice and, perhaps, unhelpful because of data overload. From a fairness standpoint, legislative proposals lack any comparable requirement that government entities share threat information with CCI.

Policymakers Should Advance Collaborative, Sector-Based Risk Assessments

Over the past year, the Chamber has developed and worked with other industry organizations on cybersecurity proposals that offer positive and cooperative approaches to increasing U.S. information security and resilience.

The Chamber believes that policymakers should leverage and improve upon the sector-based risk assessments already being conducted by DHS or sector-specific agencies and industry under the existing NIPP. A key premise behind advocating collaborative sector-based risk assessments is to help answer a question that policymakers frequently ask: How are we doing on cybersecurity? Unfortunately, this question leads some to want to regulate the businesses community in prescriptive and unhelpful ways.

The Chamber has written a proposal advocating that DHS and industry sectors routinely produce a sector or subsector risk assessment that paints a picture of the strengths and vulnerabilities of the sector's cyber preparedness and resilience against a significant disruption, such as a cyberattack or a natural hazard. In contrast, the bill seems to use sector assessments as a springboard to increased regulation, rather than toward greater collaboration. Policymakers should ensure that the private sector and the federal government have done nearly everything they can within the public-private partnership framework to enhance U.S. cybersecurity before making a leap to an uncertain regulatory program.

Let's Boost Public Awareness

For several years, the Chamber has partnered with DHS and other agencies to increase businesses' knowledge of cybersecurity from an enterprise risk-management perspective. The Chamber has also promoted *Stop. Think. Connect.*, a public-private education and awareness campaign to help people stay safer and more secure online. But more needs to be done. We recommend heeding the example of government and industry mobilization in 2009 to halt the spread of the H1N1 flu virus. Simple and effective resources were made available to households, businesses, and schools across the country to mitigate the impact of the outbreak.

This collaborative effort could serve as a model for stemming much of the nefarious and comparatively unsophisticated activity seen online, freeing up limited human and capital resources to focus on more advanced and persistent threats. The Chamber recently partnered with the Federal Communications Commission (FCC) to unveil the FCC's new *Small Biz Cyber Planner*, a free online tool to help small businesses protect themselves from cybersecurity threats and make the price of attacks steep for their digital adversaries.

The Way Forward: Congress Should Enact a Meaningful Information-Sharing Bill

Cybersecurity is a significant economic and national security issue that the Chamber takes very seriously. We believe that the right path forward is for the public and private sectors to work together to solve challenges, to share information between network managers, and foster investment and innovation in cybersecurity technologies. The optimal way forward will not be found in layering additional regulations on the business community. New compliance mandates would drive up costs and misallocate business resources without necessarily increasing security.

Critical infrastructure owners and operators devote significant resources toward protecting and making resilient their information systems because it is in their overwhelming interest to do so. The Chamber urges Congress to support efforts that genuinely enhance collaboration between industry and government partners.

In addition, the Chamber supports information-sharing legislation that would address the need of businesses to receive timely and actionable information from government analysts to protect their enterprises by improving detection, prevention, mitigation, and response through enhanced situational awareness. The legislation should build on the recent defense industrial base (DIB) pilot project as a potential model for demonstrating how government cyber threat intelligence can be shared with the private sector in an operationally usable manner.

Businesses need certainty that threat information voluntarily shared with the government would be exempt from public disclosure and prohibited from use by officials in regulatory matters. Legislation needs to provide legal protection for companies that guard their own networks in good faith or disclose cyber threat information with appropriate entities, such as ISACs.

Once again, the Chamber greatly appreciates the opportunity to testify today. We look forward to working with you on these and other issues. Thank you very much.

Securing America's Future:
The Cybersecurity Act of 2012

Statement of Stewart A. Baker
Partner, Steptoe & Johnson LLP
Visiting Fellow, Hoover Institution, Stanford University

Before the Homeland Security and Governmental Affairs Committee
United States Senate

February 16, 2012

Mr. Chairman, Ranking Member Collins, members of the committee, it is an honor to testify before you on such a vitally important topic. I have been concerned with cybersecurity for two decades, both in my private practice and in my public service career, as general counsel to the National Security Agency and, later, to the Robb-Silberman commission that assessed U.S. intelligence capabilities on weapons of mass destruction, and, more recently, as assistant secretary for policy at the Department of Homeland Security. In those two decades, security holes in computer networks have evolved from occasionally interesting intelligence opportunities into a full-fledged counterintelligence crisis. Today, network insecurity is not just an intelligence concern. It could easily cause the United States to lose its next serious military confrontation.

Moore's Outlaws: The Exponential Growth of the Cybersecurity Threat

Our vulnerabilities, and their consequences, are growing at an exponential rate. We've all heard of Moore's Law. What we face today, though, are Moore's outlaws: criminals and spies whose ability to penetrate networks and to cause damage is increasing exponentially thanks to the growing complexity, vulnerability, and ubiquity of insecure networks. If we don't do something, and soon, we will suffer network failures that dramatically change our lives and futures, both as individuals and as a nation.

It doesn't take a high security clearance or great technical expertise to understand this threat. It follows from two or three simple facts.

Fact One. Breaking into computer networks to steal secrets has never been easier, despite all the security measures we encounter on those networks.

Why do I say that? Simple. In recent months, we have learned that some of the most security-conscious institutions on the planet have been compromised. HBGary, RSA, Verisign, and DigiNotar are all in the network security business; they understand how to protect secrets on line -- if anyone does. But RSA was electronically attacked and its most important business secrets, the keys to its security business, were stolen. HBGary lost control of its CEO's email correspondence to a group of online vigilantes, and its CEO lost his job as a result. DigiNotar, a Dutch entity that issues online credentials, was compromised by a hacker working with Iranian security forces. Six weeks after the breach became public, DigiNotar was out of business. I

think it's fair to say that these security-conscious companies would have done whatever they could to prevent these disclosures, but they failed. They were unable to secure their networks.

Actually, the same is true for governments. The Defense Department used to say that attacks on its systems had never penetrated the classified networks. Now it has disclosed that this is no longer true. Defense contractors have also been compromised, and with them, the designs for our most recent weapons systems.

That is the first fact: No network, no matter how important its secrets and no matter how security conscious its owner, can be seen as secure in today's world. Attackers have an excellent chance of breaking in and stealing secrets. And here is the second:

Fact Two. Once the attackers are in, they don't have to stop at stealing secrets. They can cause severe physical damage just by manipulating the digital systems they have compromised.

When I was at DHS, we demonstrated that hackers could cause a large generator to self-destruct, just by sending the generator commands over the network. More recently, the Stuxnet malware is believed to have crippled Iran's uranium enrichment efforts for months, simply by infecting the computerized industrial control system responsible for Iran's centrifuges. That was good news for people who think that Iran's nuclear program is dangerous. But Stuxnet was also a proof of concept, showing that network flaws can be used to cause massive damage to any machinery that relies on computerized industrial controls.

And what machinery runs on such controls? Pretty much everything necessary to sustain our society: refineries, pipelines, electric power, water, and sewage systems. Worse, the industrial control systems that run these necessities are not really designed with cybersecurity in mind. In fact, there is reason to believe that Windows networks running on the Internet are much more secure than industrial control systems. At a minimum, we can say with confidence that industrial control systems are no better protected than the systems that failed at RSA, Verisign, HBGary, and DigiNotar.

Cyberweapons pose a real threat to the United States. Those two facts lead to a third, common-sense conclusion: Any nation that feels the need to prepare for a military confrontation with the United States has already begun developing cyberweapons. Cyberweapons are especially potent against the United States. That's because they are deniable; figuring out who has launched a cyberattack will be very difficult, making our other military assets less useful in deterring attacks. Cyberweapons are also asymmetric; they cause more harm in developed nations than in less advanced societies. And perhaps most importantly, such weapons can overturn the American war experience of the last sixty years – that conflicts will be fought far away, at a time and place of our choosing. Any nation expecting a conflict with the American military would be enthusiastic about developing a weapon that can cause massive civilian suffering on our home front before a single shot has been fired on the battle lines.

Now that such a weapon is within their reach, the impact could be unprecedented. We have no experience with losing large parts of our power, refinery, water and sewage systems all at once. The closest we've come was New Orleans after Katrina. And there, everyone knew beforehand

that the disaster was coming. Preparations had been made, and most people left the city well in advance. They went to places where the infrastructure still worked, while organized military and civilian relief efforts rapidly moved in to help those who remained. Even so, the breakdown in order and the human suffering was extreme.

Thanks to growing cyber insecurity, all Americans now live in a digital New Orleans, with Katrina just offshore. And not one Katrina, but many. Computer exploits that we once thought were the work of large nations such as Russia or China now seem to be within the capability of countries like Iran and North Korea. If I am right that computer insecurity continues to grow worse each year, then the sophistication needed to launch a cyberattack will continue to decline, and soon such attacks will be within the capability of criminal gangs and online vigilantes like Anonymous.

Disaster is not inevitable. We can head this threat off if we treat it seriously. We may have years before suffering an attack of this kind. We do not have decades. We must begin now to protect our critical infrastructure from attack. And so far, we have done little.

The Cybersecurity Act and Its Critics

The committee and the bipartisan group that has worked with the Majority Leader deserve great credit for producing a historic comprehensive legislative package to deal with this grave threat. The bill does three big things. First, it seeks to improve the cybersecurity of the infrastructure industries on which our lives and social order depend. Second, it sets aside the legal restrictions and doubts that have made it hard to share security information between government and industry. And third, it reforms the federal information security standards process.

Of these, the most important is the title dealing with critical infrastructure, and I will focus my testimony on it. This part of the bill will no doubt encounter resistance. The business community is quick to condemn anything that smacks of new government regulation. Information technology companies have achieved enormous success in recent decades and have gone largely unregulated. They want to stay that way.

They argue that information technology is too fast-moving and technically complex for government to regulate. And that's not completely wrong. It is a fool's errand to address network vulnerabilities by adopting command-and-control regulations specifying particular security measures. A new regulation takes two to three years to wend its way through notice and comment and other mandated procedures. In three years, malware will go through several generations, and attacks will evolve many times. Specifying particular security measures by regulation will not work.

But neither will *laissez-faire* reliance on the private sector. We do not expect General Motors to field its own antimissile defenses in the event of a nuclear attack. And we cannot expect private power or oil companies to stand alone against calculated attacks from the militaries of half a dozen nations. I believe that the bill, with a few modifications, charts a way to improve private sector security without resorting to command and control regulation.

Another source of resistance comes from advocates who claim that this bill is somehow similar to the Stop Online Piracy Act, or SOPA. If the bill reaches the floor, they threaten, it will meet the same fate as SOPA.

Well, to paraphrase Sen. Bentsen in the 1988 vice-presidential debate, I knew SOPA, I opposed SOPA, and Mr. Chairman, this bill is no SOPA.

I took a very early stand against SOPA, and I'm proud to have played a role in forcing its reconsideration. SOPA was a bad idea because it would have given a little help to one industry while making everyone who uses the Internet much less secure. That criticism of SOPA struck a chord with Americans because we all use the Internet with a nagging fear that our security is at risk. That security concern was at the heart of the early opposition to SOPA. This bill, in a real sense, is the opposite of SOPA. It addresses the entirely justified security concerns of ordinary users.

There is another reason not to heed the advocates who oppose this title. They're the guys who got us into this fix.

Three Presidents in a row have warned against cybersecurity risks, and three have tried to do something about it. All have been stymied by business and privacy advocates acting in alliance. A dozen years ago, President Clinton's administration proposed that the Defense Department build tools to check Internet traffic sent to DOD sites, not just for spam but for malware that might be sent by foreign governments. In response, business and privacy groups rose up, claiming that this would somehow violate the rights of people communicating with the government. The proposal was killed in Congress. Today, after what may be the most massive loss of weapons technology and other secrets in history, we are only beginning to build an Einstein system that does for civilian systems what President Clinton was not allowed to do.

We've had a lost decade in cybersecurity. The government bears some responsibility for that lost decade, but those who counsel inaction bear more. We followed their advice, and the threat is far worse now than it was ten years ago. If we follow their advice again, we will face a crisis much sooner.

Unpacking the Critical Infrastructure Protection Proposal

In fact, if I may turn to the contents of the bill, I fear that it has already been weakened unduly by those who want us to do nothing.

That is not to criticize the overall thrust of the bill. The title on critical infrastructure is in general a well-considered and coherent approach. It starts with a government assessment of the industries where the risk is greatest. See section 102. Based on the assessment, individual systems or assets deemed to be most at risk are, on an industry sector-by-sector basis, designated as "covered critical infrastructure." Section 103. Next, performance requirements to mitigate those risks are adopted for each industry. Section 104. Finally, adherence is enforced by requiring the owner of covered infrastructure to certify compliance (or to obtain a third-party assessor's certification of compliance) with the performance requirements. Section 105.

This broad structure is meant to solve the problem of how to regulate a fast moving and complex technology. It does so by leaving as much discretion as possible in the hands of the private sector. It gives the private sector preferential input into the process of assessing and identifying covered critical infrastructure. Performance requirements are supposed to be established, if at all possible, based on private sector proposals or existing industry standards. What's more, the title doesn't call for government simply to tell industry what security technologies to adopt. The point of the process is to identify the risks, warn industry of those risks, and challenge industry to develop standards and adopt measures that industry finds best adapted to the risks.

Done well, an approach of this kind is both more demanding and more flexible than traditional regulation. The government sets the bar, and it is up to industry to find the best way to get over it. That makes the approach more flexible than ordinary regulation. But if hackers find new ways to compromise critical networks, then industry measures that once were good enough must now be strengthened, automatically and without a new regulation. That makes the system more demanding than ordinary regulation. It's a good solution.

In several details, however, the bill fails to follow through on its overall approach.

How many deaths does it take before security matters? First, because the bill imposes no obligations whatsoever on systems or assets that are not designated as "covered critical infrastructure," the process of designation is a big deal. If an asset is not designated as "covered critical infrastructure," then the owner has no obligation under the bill to guard against attack by hackers, criminals, or nation states, leaving those who depend on the asset unprotected. So, the standards for prioritizing industries and designating systems or assets are crucial.

Yet the standards currently included in the bill for designating "covered critical infrastructure" are bound to leave huge swaths of important systems unprotected. The bill states that the Secretary of Homeland Security may "only designate a system or asset as covered critical infrastructure if damage or unauthorized access to that system or asset could reasonably result in . . . (i) the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause (I) a mass casualty event that includes an extraordinary number of fatalities; or (II) mass evacuations with a prolonged absence; (ii) catastrophic economic damage to the United States . . . or (iii) severe degradation of national security of national security capabilities, including intelligence and defense functions. "

Let's unpack that first test. It says that a system or asset cannot be regulated under this bill unless a cyberattack on it would so interrupt life-sustaining services that it would cause "a mass casualty event that includes an extraordinary number of fatalities." Really? So an individual infrastructure owner, such as a rural electricity provider, has no responsibility under this title if it can show that an undefended cyberattack would only cause an *ordinary* number of fatalities?

How many dead Americans is that, exactly? Under the bill as written, any business that wants to avoid being regulated can take the government to court and argue that it is exempt from obligation under the law because only a few its customers will actually die if its security fails. That's wrong. The courts are going to have to give effect to every adjective in this bill, from

"extraordinary" numbers of fatalities, to "catastrophic" economic damage and "severe" degradation of national security. Do we really want to see companies escape any security obligations by arguing that their failures will of course degrade national security or cause economic damage, but not severe degradation or catastrophic damage? This would be a better bill if those adjectives were reconsidered.

The information technology exclusions. My second concern is that the bill gives the IT industry too much of a free pass. The bill expressly prohibits the inclusion of any "commercial information technology product, including hardware and software" within the category of "covered critical infrastructure."

This is odd. Commercial information technology products are certainly part of the problem. Why shouldn't they be part of the solution?

Of course IT companies have legitimate concerns about how regulation would affect their ability to innovate, especially on a global basis. Perhaps it doesn't make sense to treat individual platforms, such as Windows, as covered infrastructure sectors. But at the same time, we cannot ask the owners of covered networks to improve security without help from their IT providers.

The bill as drafted probably does allow the government to set standards for IT companies indirectly. (Thus, the government could endorse a performance standard like this one: "Operating systems utilized by covered critical infrastructure must enable authentication of each machine on the network by means of a trusted processing module or equivalent hardware-based technique.") Assuming this is consistent with the statute, the exclusion of commercial IT products from covered infrastructure may be tolerable.

But such an indirect approach is put at risk by a second set of limits written into the bill. These exclusions would prevent the government, when establishing performance requirements, from requiring the use or regulating the design of commercial information technology products and related services. This language is much too broad. It would cast doubt on any performance standard that applies by its terms to commercial hardware or software used by critical industries, including the example that I gave above.

It seems to me that, if IT products are not to be treated as a covered infrastructure, the companies that make them should be encouraged to provide very specific forms of security support to those of their customers who are covered. Put another way, the IT industry can reasonably ask for one of these exclusions, but not both.

Immunity for operators who have no statutory obligations. By the same token, the bill imposes obligations on the owners of critical infrastructure but not on the operators of critical infrastructure. This seems to exclude anyone who acts as an outsourced provider to the actual owner. So if a telecommunications company outsources its hardware operation to a foreign switch manufacturer or a pipeline company hires an IT company to run its networks, the obligations of the bill do not apply to the switch manufacturer or the IT company. This is less troubling, I suppose, than the blanket exclusion of all commercial IT products, since obligations

imposed on the owner may be passed on to the operator. But if the operator isn't subject to regulation, why should we reward the operator as well as the owner with an immunity from punitive damages?

Cutting through the regulatory drag in an emergency. Finally, my biggest concern about the bill has to do with the risk of regulatory atherosclerosis. The process set forth in the bill is very friendly to industry, deferring at every turn to industry-led standards and solutions. In general, this is a good idea. But the end result is a process that will take many years to implement, especially in sectors that decide to resist rather than comply with the intent of Congress.

Here's my quick assessment of the likely elapsed time from enactment to actual implementation of security measures by a reluctant industry.

- **Risk assessments.** The top-level risk assessment must be done in 90 days, but there is no deadline for doing sectoral risk assessments. Those could take at least a year and probably two to finish, and they must be completed before the remaining steps can be taken.
- **Designation.** The government must explain its criteria for designation, and it appears that it must individually identify the companies to be designated. What's more, every decision it makes can be challenged in court, which will make the government cautious and slow in making designations. This step too will take at least a year or two in many sectors. And that's not the end. The bill chooses the slowest possible judicial review process, sending appeals first to district court and then up on appeal. Any industry that appeals its status could buy two or three more years before the next step can be taken.
- **Set performance requirements.** The bill's preferred method for setting performance requirements is to rely on stakeholder proposals or existing industry standards. But if, after all of these proposals are submitted and reviewed, they are insufficient to address the security threat at issue, then and only then can the Secretary of Homeland Security, still in consultation with industry, develop satisfactory requirements. That process too could easily take another two years.
- **Enforce the requirements.** Once all of that is done, and an enforcement regulation has been written, each covered company must certify that it has adopted measures that it considers sufficient to meet the applicable performance requirement. (Alternatively, the company can choose to wait for the government to go through the long process of creating, training and testing up an entire new class of third-party assessors.) If the government suspects that the company's certification is false, it can conduct its own assessment, but it's not completely clear that it can impose any new requirements; it may be that the company can wait to be sued for a false certification and then avoid any penalty by adopting a new set of security measures and claiming that it has remediated any failure in a timely way. That could be very lengthy and messy, but let's figure a year for the certification and another year to sue a recalcitrant company.

Based on those calculations, a company that simply exercises rights conferred by the title could delay any cybersecurity measures for eight to ten years after enactment. That's another lost decade.

I don't mean to suggest that the risk of delay should be solved by getting rid of these lengthy processes. They are necessary to get the benefit of the private sector's creativity and flexibility in dealing with security problems. They should be retained in most circumstances.

But clearly there are some problems that we cannot wait a decade to solve. In an emergency, the government must have authority to skip or compress any of the procedures described above. If a security threat to a particular company or sector plainly threatens the lives of Americans, the department should be free to demand prompt action by the company. The company may remain free to choose the solution, but the government must be able to insist that the solution work and that it be implemented as promptly as necessary to save lives. That, after all, is the purpose of this bill. Without authority to waive time-consuming procedures in an emergency, the bill will fail in that purpose. I know such authorities are hard to draft, so I've attached one possible version to my testimony.

Conclusion: Our Best Hope to Avoid a Predictable Disaster

In closing, let me return to my main theme. We face a crisis. Cybersecurity is bad and getting worse. Civilian lives, and our ability to win the next war, depend on solving our security problems. We have to do that without losing the great benefits that a largely unregulated global IT industry had brought to us. But we cannot let advocates for the status quo condemn us to another lost decade of growing insecurity. This bill, even with its flaws, is our best hope to head off a perfectly predictable disaster.

We are all living in a digital New Orleans. No one really wants to spend money reinforcing the levees. But the alternative is worse.

And it is bearing down on us at speed.

Possible Amendment to Deal with Imminent Threats

Stewart Baker

SEC XXX. RESPONDING TO IMMINENT THREATS

(a) Notwithstanding the other sections of this Title, in the event that the imminence or existence of a cybersecurity emergency as defined in section (b) makes it impracticable to complete one or more of the steps below in accordance the procedures established under this title the Secretary shall have the authority to promptly —

(1) identify cyber risks that have created the cybersecurity emergency within one or more affected sectors;

(2) designate the covered critical infrastructure and any systems or assets that must respond to these risks;

(3) develop risk-based cybersecurity performance requirements that address the identified cyber risks;

(4) require, within a period of time determined by the Secretary, that each owner of covered critical infrastructure, whether identified under this section or section 103 of this title, implement security measures sufficient to satisfy the risk-based security performance requirements established under this section and promptly —

(A) certify in writing to the Secretary that the owner has developed and effectively implemented security measures sufficient to satisfy the risk-based security performance requirements established under this section; or

(B) submit a third-party assessment in accordance with Section 104(d);

(5) enforce any requirement of this section; and

(6) expedite the implementation of any other provision of this title.

(b) The Secretary shall declare that a cybersecurity emergency exists only when a cybersecurity risk to a particular critical infrastructure sector --

(1) cannot be prevented in timely fashion by adhering to the procedures set forth in sections 102 through 107 of this title; and

(2) poses a present or imminent threat of

(A)the interruption of life-sustaining services, including energy, water, transportation, emergency services, or food, sufficient to cause—

(i) a mass casualty event that includes an extraordinary number of fatalities; or

(ii) mass evacuations with a prolonged absence;

(B) catastrophic economic damage to the United States including—

(i) failure or substantial disruption of a United States financial market;

(ii) incapacitation or sustained disruption of a transportation system; or

(iii)other systemic, long-term damage to the United States economy; or

(C) severe degradation of national security or national security capabilities, including intelligence and defense functions.

(c) Judicial review in accordance with section 103 shall be available as provided in that section, but no stay shall be granted of any order, determination, directive or other action under this section unless the party requesting the stay posts a bond fully sufficient to cure any harm that may be caused by failure to implement the stayed order, determination, directive, or other action.

Testimony
U.S. Senate Committee on Homeland Security and Governmental Affairs
Thursday, February 16, 2012,
"Securing America's Future: The Cybersecurity Act of 2012."
James A. Lewis, Center for Strategic and International Studies

Mr. Chairman and members of the Committee, thank you for the opportunity to testify. Congress has an important and defining challenge before it as it considers cybersecurity. This technology has profound implications for our economy and for our security, but law and public policy have not kept up. The laws and policies that were appropriate when the internet was a toy will not secure our nation as we become increasingly dependent on what has become a critical global infrastructure. We derive tremendous economic benefit from cyberspace, but it is also a source of unparalleled vulnerabilities for our nation, vulnerabilities that others have been quick to exploit.

Reducing risk and vulnerability in cyberspace is a fundamental challenge. In considering this problem, we have learned through painful experience that market forces will not secure cyberspace and that existing authorities are inadequate for national security and public safety. The list of private sector companies, including technology leaders, whose defense have failed is long and would be longer if all breaches were disclosed. Continuing to use voluntary, market driven approach to this new national security concern is irresponsible and guarantees a successful attack against our nation. The Committee has done our nation a service by taking on the challenge of cybersecurity. Unfortunately, Mr. Chairman and members of the Committee, while there are many good things in this bill in a few crucial areas it needs to be strengthened. As currently drafted, this bill includes significant loopholes that would keep our nation at risk.

Some of these loopholes are intended to accommodate industry concerns. These industry concerns are understandable and the bill makes reasonable efforts to accommodate them. However, in a few instances the language to assuage industry concerns goes too far and ends up putting national security at risk. As with any important regulation, there is a delicate balance between protecting the nation and minimizing burdens on our economy. This bill makes valuable strides in this direction and with a few changes, the Committee, the Senate and the Congress can find the balance that best serves the national interest.

In the long discussion leading up to this hearing, a number of objections have regularly been used to explain why it should be diluted or rejected. This is part of politics in a democracy and we will ultimately see truth emerge from debate. Ultimately, my hope is that we can find a pragmatic approach that protects the nation, but to do this we must hold some of the assertions about the risks of better cybersecurity up to the light and examine them more closely.

The strangest of these assertions is that we face no real threat in cyberspace, or that the threat does not warrant taking action, or that the defense industrial complex has inflated cyber threats to justify spending. Like any new trend in policy, cybersecurity has in the last few years attracted a wave of new scholars who are, in a sense, learning their trade by doing it. The field is fragile, hampered by poor data, weak research methodologies, inexperience and powerful ideologies. Cybersecurity also has a unique problem in that some of the most reliable data is classified. This

noisy debate is a symptom of the growing pains that societies experience as they adjust to a new technology. We are at an inflection point, however, when it comes to cybersecurity. The existing approach has failed and change is inevitable, either through our own efforts or after it is forced upon us by events.

I know you have been briefed by senior administration officials on the threat we face, and that those of you who have served on the intelligence oversight committees have a deep appreciation of the problem. But there are still many who either lack this knowledge or profess to be unconvinced. Even using only open source material, we can assess the growing threat to national security and public safety in cyberspace.

Many countries are building cyber-attack capabilities – a study last summer found thirty five nations developing military doctrine for cyber war. Two of the nations that are most advanced in cyber-attack capabilities are among our most likely military opponents – Russia and China. These nations bear us ill-will and their militaries and intelligence services have planned cyber-attacks against us. Barring some miscalculation, they will avoid cyber war but if there was a conflict with either nation, the U.S. is shamefully defenseless.

China and Russia are great powers with many interests and are unlikely to engage in frivolous attacks. They have instead taken advantage of our weak cyber defenses to engage in widespread economic espionage and crime. Other potential attackers may not be so restrained. When these less constrained attackers acquire advanced cyber-attack capabilities, the risk to the U.S. will increase significantly. The two most dangerous of these "acquiring powers" are Iran and North Korea, but anti-government groups, cyber criminals and perhaps jihadis may also be acquiring cyber-attack capabilities.

Iran has been seeking cyber-attack capabilities for years. We do not have a good understanding of Iranian capabilities, but Iran was probably responsible for hacking a Dutch internet company "Digi-Notar," to intercept communications from Iranian dissidents. This was a significant breach that put online commerce at risk. Iran has close military relations with China and Russia, who could assist it in developing cyber capabilities. Director of National Intelligence James Clapper testified recently that Iran is losing its reluctance to strike domestic targets in the U.S. Given its demonstrated willingness to use proxies for terrorist acts, Iran could decide that it is safe to launch a covert cyber-attack against our vulnerable infrastructure.

North Korea has been pursuing cyber warfare capabilities since the mid-1990s and Kim Jong-il, the former leader, had a deep interest in information warfare and ensured long term support for the DPRK military to acquire cyber-attack capabilities. North Korea routinely probes South Korean networks and may be responsible for several basic-level attacks. As with Iran, open source information on North Korean capabilities is limited, but we know they want cyber weapons and it is unwise to depend on the restraint of a nation that feels no compunction about shelling islands or torpedoing patrol boats.

Another potential source of cyber-attack comes from antigovernment or anarchist groups. This could include teenagers with a grudge, anarchists who wear black masks and smash shop windows in violent protests, cyber criminals, and perhaps even foreign intelligence services

attempting to use political groups as "cover." To date, most of the actions attributed to these groups have been a source of annoyance more than damage. But some in the hacker community say that some of the most skilled hackers in the world are among the ranks of Anonymous, a leading hacker group. We have some idea of their motivations, which are anti-government and anti-American, and of their inventiveness and skill, as they, like our nation-state opponents, have been able to exploit corporate networks with ease.

While the likelihood of cyber-attack is increasing, it is still unlikely that these attacks would cause mass casualties or catastrophic damage at a national or regional level. Attacks will likely resemble the Stuxnet attack, the 2003 Northeast Blackout, or the 2010 stock market "flash crash." Neither the blackout or the flash crash were caused by cyber-attack, but they were the result of computer failures and a shrewd opponent could duplicate these failures and exploit our lack of defenses to make incidents like these last weeks instead of a few days. I would note that in the Northeast Blackout, the "Flash Crash," of 2010, or even Stuxnet, there were no casualties, no mass evacuations. If we set the threshold for covered critical infrastructure as requiring mass casualties, mass evacuations, or national catastrophe, we may inadvertently be saying that we do not need to defend America against Stuxnet-like attacks.

It is important to focus new authorities on truly critical infrastructures, and to minimalize the effect of new regulation, but we should also bear in mind the nature of asymmetric warfare. When the threshold for identifying covered critical infrastructure uses terms like mass casualties, mass evacuations, or effects similar to weapons of mass destruction, we are essentially writing target lists for our attackers. They will attack what we choose not to defend. The critical infrastructure excluded from regulation will be the most likely target for attack.

Every critical infrastructure operator whose networks have been examined has been found to be vulnerable, and in many cases, examinations have found that opponents have spent months to "prepared the battlefield" for potential future strikes against America. Companies may not be aware of the threat and in any case, there are powerful and perfectly understandable economic disincentives for them to spend on public goods like national defense. We need to be cognizant of this and look for ways to allow companies to recoup costs. Not requiring them to improve their defenses, however, is a debacle waiting to happen, and better protection for critical infrastructure from cyber-attack is an immediate national concern.

We also know that America has been the victim of sustained and widespread campaigns of cyber espionage. The most technologically advanced companies in America have been no match for foreign opponents who have routinely and easily overcome private sector defenses. Companies, naturally, conceal their losses and may not even be aware of what has been taken. Government agencies, through their own activities, have an idea of what American firms have lost and have knowledge of the plans, intentions and capabilities of our most active opponents, but a welter of well-intentioned laws written in the 1980s to protect privacy hampers the ability to share this information among companies or between private sector and government. This bill, along with proposed legislation in the House, appropriately addresses the information sharing problem. This cyber espionage costs American jobs, damages trade competitiveness, and puts our technological advantage at risk.

Government agencies have also been the victim of cyber-espionage, but they have in the last few years undertaken a vigorous response that has improved their defense. The most notable examples of this is the creation of Cyber Command in response to the 2008 penetration of a classified military network and actions taken at the Department of State that have dramatically reduced opponent success rates. The section of this bill that address FISMA are important to solidify and continue this progress, but frankly, we have not seen similar progress in the private sector, where cyber defenses are uneven and exploitable.

Yesterday's Wall Street Journal's story on Nortel illustrates the problem. Hackers stole passwords form Nortel executives, including the chief executive officer. This gave them access to "technical papers, research-and-development reports, business plans, employee emails and other documents." The penetration lasted many years and Nortel "did nothing from a security standpoint" to end the penetration. We do not know how many other situations like Nortel are out there, but we do know that many Fortune 500 companies have been the victim of similar exploits.

As a nation, we are still too reliant on cybersecurity policies from the 1990s that depend on voluntary action, market forces and feckless public private partnerships. This approach has failed. It is inadequate for what has become a global infrastructure that our economy relies upon and, because of its speed and scale, makes criminals, spies and hostile militaries our next door neighbors. Continued endorsement of these old ideas as the basis for cybersecurity puts the nation at risk.

One common theme is that we need to keep cybersecurity weak to avoid damaging innovation. Innovation has become a kind of mantra in Washington, but our assessments of how to accelerate innovation are inadequate. We need a better understanding of the role of the Federal investment in education and research and its relation to the commercialization of new technologies by the private sector if we are to rebuild our innovation capacity. We need to improve the general economic environment and remove obstacles to the creation of new businesses – but there is nothing in this bill that creates such obstacles to innovation. Increasing America's ability to innovate is a serious concern, but to argue that this requires weak cybersecurity is nonsensical. Because of the ease of cyber espionage, our national spending on innovation is, in effect, a partial subsidy to foreign competitors: they share the fruits of our investments without having to pay for them.

The relationship between innovation and regulation is complex and is easily mischaracterized. Too much regulation or regulation that is too prescriptive will damage the ability of entrepreneurs to create new companies. Well-intentioned regulations, combined with badly designed fiscal and investment policies, slow American economic growth. Too little regulation, however, puts the public interest at risk. Events on Wall Street demonstrated this – America deregulated the financial sector, and then it crashed the global economy. Our current weak regulatory structure for cyber security puts us on track to repeat this mistake at the expense of national security. What is needed is a pragmatic, minimalist, and balanced approach to regulation. Finding this approach can be difficult, but the approach taken in Section 105 is, dare I say it, innovative, avoids prescriptive regulation and follows established commercial practices to create a minimalist regulatory structure that will, if the threshold for covered infrastructure

and the exclusions for commercial IT products are revised, will increase national security and serve the national interest.

In fact, well-designed regulation can spur innovation. The Federal Aviation Administration has far more intrusive and onerous regulation than what is envisioned in this bill. The FAA was established in 1958, but we have been able to move beyond propeller aircraft. Similarly, when car manufacturers testified decades ago before Congress on auto safety regulation, they said that Federal intervention to make cars safer would destroy the American auto industry. The American auto industry has had several near death experiences since then, but these have been self-generated rather than the result of burdensome regulation. Auto safety regulation created a competition among car manufacturers to innovate in building new safety feature. Regulation accelerated innovation in this case while saving thousands of American lives.

Some might say that aviation safety is more important than cybersecurity, but as the internet and digital applications move to the center of economic activity, this would be a grievous mistake. National security and public safety are burdensome, and can require burdensome regulation. But we should not pretend that avoiding the burden will somehow make us safe. There is a natural tendency in this discussion to exaggerate the costs of cybersecurity. Most studies of cost are regrettably inaccurate. Better cybersecurity may not entail any new cost, just change in how people spend. This would not be true, of course, if a company is currently spending little or nothing to secure its networks, but isn't this the problem we are trying to fix?

One question that comes up repeatedly is that we regulate flight and autos because a failure to do so would result in death, but we will not have cybersecurity regulations until someone dies. Many in the security and intelligence world believe we will not take cybersecurity seriously until there has been a disaster. This Congress has an opportunity to prove them wrong.

Some privacy advocates oppose stronger cybersecurity measures. The heart of this opposition is a distrust of government and a fear that new authorities will be misused. These are, frankly, reasonable concerns that can only be addressed by adequate oversight and clear rules and limits on how new authorities can be used. This oversight responsibility falls first on the Executive Branch and bodies such as the President's Civil Liberties Oversight Board, which is moving steadily towards realization, but ultimately it is the responsibility of the Congress. The measures in this bill, frankly, do not pose any real risk to privacy or civil liberties, but the legacy of Warrantless Surveillance continues to raise concerns that can only be addressed by a strong commitment to oversight and transparency.

There is a question of how far "upstream" in the industry DHS should have authority. Section 104 of the bill excludes all commercial software and hardware. I am not sure what this would leave, as I know of no freeware or open source industrial control systems or microprocessors. We do not want agencies telling Information Technology companies how they should write code, but carving out all "commercial IT products" risks seriously undercutting the positive effect of the bill.

Section 104 needs to be clarified to ensure that owners and operators of covered infrastructure can be required to mitigate identified vulnerabilities. In particular, it needs to clarify that

existing guidelines on vulnerabilities can be applied to critical infrastructure networks. The intent of Section 104 is understandable. It seeks to shield the commercial information technology vendors from regulation and liability. Section 104 (b) (2) (c) makes sense. DHS should not be telling companies how to write code or design semiconductors.

But as drafted, the section seriously weakens the bill. It basically says that the Federal government cannot regulate or require any changes in commercial information technology, how it is installed, or how it is maintained. If commercial information technology products currently in use were secure, were installed securely and were maintained in that condition, this language would not be a problem. However, this is not the case. The blanket restrictions found in Section 104 (b) (2) (a) and (b) that forbid Federal agencies from regulating "related services, including installation services, maintenance services, repair services, training services, and any other services provided in support of the product" should really be called the "Huawei exemption." Installation, maintenance, and repair are prime attack vectors. Excluding these services from regulation is an open invitation to our most dangerous opponents.

An example of this problem was found in 2010 by security researchers examining smart grid technology. Smart grids will transmit information about consumer energy use and allow for better management of energy flows. Smart grid meters will encrypt information to protect it. One element of the encryption system would use a "random number generator," to scramble data. These are a standard element in many encryption programs. But random number generators are hard to create and can be expensive. So instead, the designers of some smart grid meters chose to use a fixed list of numbers from which the meter would randomly draw, a kind of poor man's random number generator. Unfortunately, astute teenagers could defeat this kind of encryption feature as early as the 1990s. But under Section 104, no federal agency or officer could ask for it to be changed or fixed.

You can get a sense of this by applying our FAA comparison. If this language applied to the FAA, it could not require an airline not to buy defective parts. It could not set the standards by which an airline would need to maintain its aircraft. If it learned of a problem, it could not require airlines and their suppliers to fix it. This is no way to run an airline and it is no way to defend a nation.

The effect of this language goes beyond critical infrastructure. It may undercut an important achievement from the Bush Administration in cybersecurity. Work at the U.S. Air Force found that secure operating systems settings would protect its networks against most cyber-attacks, as well as reduce cost. The Office of Management and Budget learned of this and issued a memorandum for other agencies to adopt this "Federal Desktop Core Configuration" - FDCC. Although the FDCC reduced cost and improved security, it was opposed by several IT companies and associations on the grounds that they were not adequately consulted and that the changes to a secure configuration would be costly. The objections slowed moving to more secure networks and the language in this section could have the effect of undoing or blocking the improvements now being used by Department of Defense and other agencies.

What exactly is the fear? If it is to avoid having DHS tell companies how to build their products, this is a reasonable concern that subsection c of the bill adequately addresses. If it is to avoid

liability for selling insufficiently secured products, this too is a long-standing industry concern that should be assuaged. But we need to find ways to restrict Federal interference in design and production and avoid creating new sources of liability without destroying the bill.

We do not want to limit the ability of the Federal government to establish standards for services in support of commercial technology used in critical infrastructure, including installation services, maintenance services, repair services, training services, and any other services provided in support of the product. Misconfiguration at the time of installation is a common problem and can create major vulnerabilities. Similarly, an opponent could use the remote update and maintenance services that are routinely provided to disrupt services or damage machinery. This is a real risk. This provision of the bill leaves the door open to disrupt critical infrastructure.

The Bush Administration's FDCC was just one of a number of developments in cybersecurity in the last few years that allow us to move a quantitative approach, where we can measure the effectiveness of security measures and significantly reduce risk. Anyone who tells you that we do not know how to do cybersecurity is sadly out of date. The National Security Agency, the National Institutes of Standards and Technology, and other Federal agencies are pioneering techniques that can strengthen America's defenses. But while we can require implementation and measure the rate of implementation in the Federal government, there is no comparable ability to measure and secure commercial critical infrastructure. This remains the single largest vulnerability for America in cyberspace. We still rely on haphazard policies and laws developed in the 1990s when the cyberspace was less important, critical infrastructures less vulnerable and the threats we faced smaller and the opponents less skilled.

This bill has much that is good in it. Other sections, on education, information sharing, research, international cooperation, and on how the Federal government secures its systems all make important contributions. Each deserves to be passed. But by themselves, or packaged together as a basket of low hanging fruit, they are inadequate to meet the risks we face today. The objective we all share of making America safer and more secure is in sight. Nonetheless, if this bill does not provide adequate authorities to mandate better cybersecurity in critical infrastructure, America will face increasing risk and an increasing probability of damaging cyber-attack.

I thank the Committee and will be happy to take any questions.

7

Written Testimony of
Scott Charney
Corporate Vice President, Trustworthy Computing, Microsoft Corporation

Before the
Senate Committee on Homeland Security and Governmental Affairs
Hearing on "Securing America's Future: The Cyber-Security Act of 2012"

February 16, 2012

Chairman Lieberman, Ranking Member Collins, and members of the Committee, thank you for the opportunity to appear today at this important hearing on cyber-security. My name is Scott Charney, and I am the Corporate Vice President for Trustworthy Computing at Microsoft. I currently serve on the President's National Security Telecommunications Advisory Committee (NSTAC), and I previously served as one of the co-chairs for the Center for Strategic and International Studies (CSIS) Commission on Cyber-security for the 44th Presidency.

Prior to joining Microsoft, I was Chief of the Computer Crime and Intellectual Property Section in the Criminal Division of the United States Department of Justice. During my government service, I oversaw every major hacker prosecution in the United States from 1991 to 1999, worked on major legislative initiatives, and Chaired the G8 Subgroup on High-Tech Crime and other international efforts.

Cyber-security is an important issue for America, other nations, the private sector, and individuals. I have had the privilege of testifying before Congress about cyber-security several times[1]. In an effort to better understand the challenges we face, I regularly engage with government leaders from around the world, security-focused colleagues in the IT and Communications Sectors, and companies that manage critical infrastructures. Based on these interactions, it is my opinion that cyber-attacks have joined terrorism and weapons of mass destruction as one of the new, asymmetric threats that puts the U.S., its allies, its corporations, and its citizens at risk. I commend this Committee and the members of the Senate for your continuing commitment to addressing one of America's most complex national and economic security challenges. You and your staff have created a venue for private sector input into deliberations on cyber-security, which is essential given that the private sector owns and operates most of this country's critical infrastructure.

[1] Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act" Before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on "Reviewing the Federal Cybersecurity Mission" (March 10, 2009).

Scott Charney Corporate Vice President, Microsoft Corporation's Trustworthy Computing "Securing America's Cyber Future: Simplify, Organize and Act" Before the House Committee on Homeland Security Sub-Committee on Emerging Threats, Cybersecurity, and Science and Technology Hearing on "Reviewing the Federal Cybersecurity Mission" (March 10, 2009).

It is my view that the current legislative proposals provide an appropriate framework to improve the security of government and critical infrastructure systems and establish an appropriate security baseline to address current threats. Furthermore, the framework is flexible enough to permit future improvements to security – an important point since computer threats evolve over time.

My testimony will begin with a brief discussion about the transformative effect of the Internet, as well as the challenges facing policymakers. Then I will discuss the three key outcomes that U.S. national policy and legislation should promote to improve resiliency in the near-term, and ensure continued innovation and leadership in the long-term. These three outcomes are:

1) Flexible and agile risk management, narrowly focused on risks of greatest concern and optimized to adapt to rapidly changing threats;

2) Innovative information sharing, targeted to address specific challenges and enable advanced risk management, response, and recovery capabilities; and

3) Meaningful and attainable international norms for the security of cyberspace.

The Transformative Challenge of Cyber-Security

The Internet continues to transform America and the world, with both positive and negative effects. Its decentralized architecture, open standards, and extensibility have created a global platform for communication, commerce, and innovation. Indeed, the United States is perhaps the best example of how the Internet can enhance productivity and commerce, as well as enable new forms of social and political engagement.

At the same time, today's Internet has a thriving underground economy with its own specialized roles and needs. For example, researchers may helpfully identify new product and system vulnerabilities, only to have cyber criminals use that research to develop and launch malicious code causing significant harm. We have also seen a rise in social engineering; attackers trick trusted employees into opening infected email attachments thereby planting malware on targeted systems. We have also seen attacks against the "trust mechanisms" designed to ensure security across the Internet ecosystem, such as the attacks against companies that provide security certificates for machine-based authentication and safer web browsing. Whether these bad actors are engaged in crime, economic espionage, or military espionage, or are otherwise supporting military objectives, the salient point is that governments, enterprises, and Internet citizens face an environment where cyber risks are often hard to understand and manage.

To respond effectively, the United States must integrate and harmonize its cyber policies, recognizing that actions taken by the United States Government will have ramifications beyond its own borders. The United States must ensure that its cyber policies are technology neutral and do not stifle innovation; and it must promote meaningful and cost-effective risk management

techniques and adapt them to the unique nature of cyber risks. Success in the long-term will also ultimately depend on building a workforce – and future leaders – for the Information Age.

The need to integrate and harmonize cyber-security policies is, in part, a byproduct of the Government's progress in cyber-security. In prior testimony to Congress on cyber-security, I highlighted the need for a national cyber-security strategy that aligned all elements of national power: economic, diplomatic, law enforcement, military, and intelligence. I further stated that the strategy must articulate how those elements would be employed to ensure national security, economic security, and public safety, and to assure delivery of critical services to the American public. At that time, the body of U.S. cyber-security policy was relatively thin.

Over the past few years, the Government has moved incrementally to improve its cyber-security posture. First, the Comprehensive National Cybersecurity Initiative set the baseline for American operational and strategic readiness, and we have since seen an array of policy documents that chart a course ahead. The White House's International Strategy for Cyberspace and National Strategy for Trusted Identities in Cyberspace, the Department of Defense's Strategy for Operating in Cyberspace, and the Commerce Department's efforts on privacy, cyber-security, intellectual property, and the global free flow of information demonstrate the Government's commitment to driving cyber-security policy forward in the right direction.

However, we have not always seen alignment or harmonization between these different strategies. While each initiative has value, their long-term effectiveness would be improved by an articulation of common goals and operational alignment to maximize their impact. It is clear that cyberspace demands a different type of policymaking; agencies cannot develop and implement policies in silos. Nor can national governments act alone. The Internet is truly global and the U.S. Government must be cognizant that American cyber-security efforts reverberate beyond our borders. In some instances, foreign governments will act in alignment with American interests and may even emulate its policies. In other instances, however, there may be disparate national approaches. Countries may have philosophical differences, of course, but sometimes technical requirements – even if promoted in the name of national security – are really attempts to create trade barriers. Policymakers must be mindful of the global import of their actions and ensure that competing interests are balanced appropriately.

More specifically, America must set an example and define cyber-security policies that are technology-neutral and do not stifle innovation. Technology-neutral policies do not promote, require, or otherwise advance a particular technology product or set of products to the exclusion of others; rather they identify desired outcomes and allow the marketplace to find the most innovative way to achieve those outcomes.

To meet these challenges ahead, the Government must catalyze the growth of leaders who can drive excellence in cyber-security. By providing new incentives for STEM education, particularly security-focused education, the Government can ensure that America has the talent necessary to be a leader in technology, innovation, and policy. Title IV in the current legislative proposal recognizes this need and initiates actions across the Federal government, academia, and industry to drive improvements. The future workforce must be able to address cyber risk management in the public and private sectors, as well as serve the needs of law enforcement and

intelligence. Moreover, we need a diplomatic corps and policymakers that grasp technology, as well as its impacts in the evolving geopolitical landscape in cyberspace.

Flexible and Agile Risk Management

Globally, governments, enterprises, and individuals depend on the information infrastructure and the data that IT systems contain, and there are often no alternative physical means to perform core functions. Yet, as discussed above, the information infrastructure faces a myriad of ever-changing cyber threats.

There is broad agreement, well reflected in various legislative proposals, that risk management is the appropriate approach to improve the security of the critical infrastructures on which we all depend. There are simply not enough resources or time to address all the risks we face. Yet while risk management is a well understood discipline, managing cyber risks is particularly difficult. This is because cyber risks are complex, it is difficult to quantify those risks and the value of potential mitigations, and it is important that we not hinder innovation and agility.

I have previously written about the challenges of understanding cyber threats and managing cyber risks,[2] so I will only summarize the key points here. While there are many malicious actors and motives, the attacks often look alike (that is, you cannot discern the actor or motive from the nature of the attack). The speed of attack may surpass our ability to respond, and responses are complicated by the fact that the Internet is a shared and integrated domain (it is shared by governments, businesses, and individuals, and the Internet is used to engage in a wide range of conduct from constitutionally protected activities to illegal acts). Finally, the potential consequences of an attack are very difficult to predict; and the worst-case scenarios are alarming.

By way of example, the market for cyber-security insurance is remarkably small, particularly given the tremendous reliance upon IT products in our daily lives. For many enterprises and even consumers, IT investments and products are at least as valuable as other assets for which insurance can be purchased. Yet, insurers are reluctant to provide coverage for cyber-incidents for a simple reason: cyber-security risk is nearly impossible to measure. The complexity, massive interconnectivity, and dependencies between systems, companies, and sectors are not well understood, and we lack sufficient data and expertise to determine with confidence the likelihood and probable consequences of a successful attack.

Therefore, while we must continue to anchor our approach to securing the information infrastructure in risk management, we must also evolve how that discipline is applied to better address the unique nature of cyber risks. When doing so, government and industry need to ensure that their approach is appropriately scoped to address pressing national security and public safety concerns, and also remains sufficiently flexible and agile to enable organizations to manage risk in a dynamic cyber threat environment.

---

[2] Scott Charney, "Rethinking the Cyber Threat – A Framework and Path Forward." http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=747 (May 3, 2010).

When considering how to effectively manage cyber risks for the information infrastructure, government must balance dual, and often interrelated, roles. First, as a public policy entity, the government is responsible for protecting public safety, as well as economic and national security and must consider which infrastructures support those missions. But the Federal government is also a large and widely distributed enterprise, with countless globally distributed customers (e.g., citizens who want to connect with their government), partners, operations, networks, and resources. Although distinct, the policy and enterprise roles are not entirely separate, as each affects and informs the other.

Government and industry must be particularly careful when delineating the elements of the information infrastructure that are truly critical to national security and public safety. While we cannot eliminate all risks, we must ensure the highest priority risks are addressed. Each risk should be assessed to determine its severity, the consequences of a successful exploit should be understood, and the likelihood of harm should be evaluated. Appropriately identifying the infrastructures that should be covered and the risks to be addressed will enable both government and private sector leaders to better secure the nation's critical information infrastructure.

Similarly, we must create a risk management framework that enables the agile responses necessary to respond to rapidly changing cyber threats. It is important to understand that risk has historically been managed by focusing on "verticals" (e.g., banking, health care) but information technology runs horizontally underneath all verticals. We therefore need a risk management model that (1) recognizes this horizontal layer (that is, IT risks need to be managed in common ways), but (2) appreciates that verticals have unique requirements. We therefore recommend a hybrid model that includes:

- A centrally managed horizontal security function to provide a foundation of broad policy, security outcomes, and standards; and

- Vertical security functions resident in individual organizations to enable them to manage their unique risks with agility.

This combination of horizontal and vertical functions ensures that minimum security goals and standards are set, yet provides organizations with flexibility to manage the unique risks associated with their operating environments.

This hybrid model is relevant to how the U.S. Government should manage cyber risk for the Federal enterprise as well as those narrow sets of systems designated as critical infrastructure. Moreover, while this hybrid model works well for both government and critical infrastructure, its implementation, and in particular the oversight and audit responsibilities, should differ. This is because the private sector has a more diverse set of business functions and, I think it is fair to say, moves at a faster pace.

The Federal government requires the hybrid model for risk management precisely because it is a large collection of businesses with different missions, partners, customers, data, assets, and risk; in other words it can and should be managed as an enterprise. While there are some responsibilities and practices that should be commonly undertaken by each and every

Federal agency, different agencies may also have unique security requirements and concerns. Thus, there should be centralized oversight to ensure horizontal requirements are established and met, as well as agency flexibility so that unique needs can be addressed.

The complexity of the IT systems and data that span and support America's critical infrastructure far exceeds that of the Federal government. Enterprises, large and small, also deliver critical functions and innovations at an unprecedented speed, and in an increasingly competitive global environment. These infrastructures are remarkable for more than their speed; their collective operations ensure public health and safety, and underpin the entire economy. Due to this fact, it is clear that critical infrastructures also have areas of commonality and areas of difference. Thus, in order to continue enabling these infrastructures to drive the economy forward, regulators should take the outcomes defined for the horizontal plane and also consider the unique implementation requirements in each sector. This approach – which does not establish a new regulatory authority – is important, as dealing with two sets of regulators would divert resources that should be devoted to security.

Having reviewed both the title seeking to reform the Federal Information Security Management Act, as well as the title focused on protecting critical infrastructure, we are encouraged to see that the proposals leverage this hybrid model, which we believe will advance security.

While appropriately tailoring the role of government, we must remain cognizant that cyber-security needs to be improved beyond just critical infrastructure. To do so, government and industry need to set the strategic context and define reasonable cyber-security goals and objectives. These objectives could form the basis of voluntary codes of conduct—a collection of recommended security goals and objectives that, if appropriately incentivized, would drive adoption of standards and widely accepted industry practices and, therefore, raise the level of cyber-security both nationally and internationally.

Innovating Information Sharing

Successful risk management depends on effective information sharing. However, over the past 10 years, several attempts to improve operational coordination between and among key government and private sector stakeholders have met with limited success. Additionally, legislative and policy efforts designed to encourage the private sector to share cyber-security information with government agencies have met with equally limited success.

That said, we—government and the private sector—have learned a lot about information sharing in the past decade, and we must apply those insights to improve the future. The paramount lesson for both the government and private sector is fairly simple. Information sharing succeeds when it is targeted at solving specific problems and challenges. Information sharing is not an objective, it is a tool, and sharing for sharing's sake is not helpful. Threats and risks are not best managed by sharing *all* information with *all* parties, but rather by sharing the *right* information with the *right* parties (that is, parties who are positioned to take meaningful action). Targeted information sharing also better protects sensitive information (whether in the

hands of the government or private sector), helps protect privacy, and actually permits more meaningful sharing of data.

Going forward, I believe that we must create two complementary information sharing capabilities, one focused on the most significant threats to national security and public safety, and another designed to enable greater automated management of IT security compliance across the federal enterprise.

The rise of the persistent and determined adversaries—whether or not state sponsored—poses ever-increasing risks. One does not need a security clearance to know that both the government and the private sector are suffering insidious and deeply damaging intrusions. Individually, organizations have visibility into only part of the problem and sometimes the damage may not be felt immediately (e.g., the harm caused by the loss of intellectual property may take time to materialize). We need new analytical approaches to tackle this pervasive threat that, if unchecked, could undermine our future economy, technology innovations, and perhaps even our national defense.

Such collaboration should be focused on the most significant threats to national security and public safety. The proposed National Center for Cybersecurity and Communications (NCCC) could, in part, provide this function and advance effective information sharing capabilities by:

- Exchanging technical data with rules and mechanisms that permit both sides to protect sensitive data;
- Analyzing the risks holistically (threats, vulnerabilities, and consequences) and developing strategies to manage those risks; and
- Developing cyber threat and risk analytics as a shared discipline.

For the NCCC to achieve success, the government needs to create the right legal environment for such information sharing and action and it must itself share information with the private sector.

In addition to increased information sharing about the most significant threats to the nation, we need to begin to address the adaptive cyber-security challenges facing both the public and private sector. Cyber-attacks can move at the speed of light or, with the right trade craft, they can unfold slowly over a protracted period of time. Through increased automation and real-time monitoring, we need to collect, analyze and disseminate information regarding attacks and develop better capabilities to respond quickly. Government and industry should collaborate so that this type of structured security automation can be used by all and, in certain circumstances, the resulting telemetry information should be shared or combined with similar data from other sources to provide a broader common view into patterns of exploit. Automation at its most basic level improves the security hygiene of an enterprise, but it can also be a foundation for sharing, analyzing, or possibly responding to potentially nationally significant events.

International Norms and Challenges

While a focus on good risk management and information sharing practices are critical, these efforts alone will not counter the global threat. We also need action internationally, and the government can help establish international norms in cyberspace.

The U.S. national security community, particularly the Departments of Defense and State, have a long history of addressing security norms in the context of nation states and military operations. In the Cold War, for example, the U.S. and Russia leveraged confidence-building measures to ensure that military exercises in one part of the world were not a precursor to a surprise invasion. In kinetic warfare, the existence of state action and the identity of the attacking state are relatively easy to determine. By contrast, cyber-attacks, even if launched against military targets, may be the work of non-state actors or individuals. The uncertainty due to lack of attribution complicates and confounds the legitimate ability of a state to respond.

U.S. foreign policy and diplomatic engagements on issues related to cyberspace security are not as focused as our efforts to combat terrorism or stem the proliferation of nuclear weapons. I believe that the U.S. must now marshal its significant diplomatic resources and expertise to advocate for cyberspace security and increase multilateral cooperation. Norms foster a shared understanding and common views that can bring a sense of order and predictability to nation-state conduct, serve as an effective way to mitigate the misunderstandings (and even conflicts) that can arise between states, and may establish ground rules for international cooperation that may help address non-nation-state actors.

I would caution that advocacy and cooperation are not goals in themselves. Like the discussion on information sharing, we need to focus advocacy and cooperation efforts toward specific outcomes. For example, working with like-minded nations to define clearly articulated norms of nation-state behavior in cyberspace could help to deter state support for cyber-attacks or hold nation-states that support such efforts accountable for their actions.

In the past year alone, the world has seen a surge in international dialogue around cyber-security norms. The dialogue has rapidly expanded from a focus on security norms, to include norms for privacy, freedom of expression, and access to the Internet. While broader dialogue and discussion on these additional topics is important, the security issues we face present somewhat unique concerns. As nations around the world continue to adopt and declare military doctrines for cyberspace, it is imperative that U.S. government focus advocacy and cooperation efforts toward specific and achievable short-term and long-term outcomes related to cyber-security.

The U.S. government should also insist that the private sector be integrated into these international discussions. Section 901 of the proposed legislation introduces some very important activities for the State Department to undertake, but it should also create a venue to integrate the views of the private sector into the formation of security norms. The private sector creates and delivers the technologies that nation states seemingly now want to exploit to promote their national interests. As a result, the private sector should be involved in domestic and

international diplomatic efforts that are intended to curb attempts to militarize the information infrastructure that it designs, deploys, and manages.

Building a consensus on what constitutes acceptable behavior in cyberspace by nation-state actors, and building a partnership among those who view the functioning of these systems as essential to the national and collective interest, is a substantial national commitment. But the return on investment would be great. Developing a global understanding of norms of behavior in cyberspace is critical to the long-term stability, reliability, and security of the Internet and the critical infrastructures upon which we all rely.

Conclusion

At Microsoft, we recently celebrated the 10-year anniversary of Trustworthy Computing, an effort created for the express purpose of driving greater security, privacy, and reliability in our products and services, as well as fostering transparency into our business practices. During the past 10 years, we have developed numerous innovations, such as the Security Development Lifecycle, which reduces vulnerabilities in our products, and the Microsoft Security Response Center, which ensures that we can respond efficiently when new vulnerabilities or attack vectors are identified. These programs have had measureable, positive impacts on the security profile of our products and services.

During this time, the market greatly enabled U.S. leadership in cyberspace. The United States is home to many of the world's most successful technology companies and one of the largest communities of Internet users in the world. But these market forces are changing dramatically and rapidly. Major emerging economic powers such as China and India are becoming centers of gravity for technology and innovation. Given that the United States will not have the same market forces at play in the future, the United States must seek other means to continue providing global leadership in cyber-security. I believe that what we have seen from Congress, in its extensive deliberations to craft a statutory response to cyber-security, provides a solid basis for continued U.S. leadership.

STATEMENT FOR THE RECORD
BY THE HONORABLE MICHAEL CHERTOFF
CO-FOUNDER AND MANAGING PRINCIPAL OF THE CHERTOFF GROUP
AND FORMER SECRETARY OF THE
U.S. DEPARTMENT OF HOMELAND SECURITY
FOR THE UNITED STATES SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENT AFFAIRS
FEBRUARY 16, 2012

I want to thank Chairman Lieberman, Senator Collins and members of the Committee for inviting me to submit a Statement for the Record and for the opportunity to contribute to this important effort that will ultimately determine how we protect our nation from today's growing and persistent cyber threat. I want to state clearly that I am submitting this Statement for the Record in my personal capacity, although, for the record, I am Co-Founder and Managing Principal of The Chertoff Group, a global security and risk management company that provides strategic advisory services on a wide range of security matters, including cybersecurity. Additionally, I am Senior of Counsel to the law firm of Covington and Burling, LLP.

The Internet as we know it today has evolved into a global system that is an essential element in our daily lives, global commerce and national security. From a remarkable technical achievement supporting a limited number of users, it is now a massive network. Because so many of our daily operations are now conducted in cyber space, they become a valuable target for daily attack by a variety of actors ranging from modern-day criminals interested in pure financial gain to nation states seeking to steal our technology or potentially to cripple our war-fighting or infrastructure. In my opinion, these cyber threats represent one of the most seriously disruptive challenges to our national security since the onset of the nuclear age sixty years ago.

But it is not my voice alone describing the importance of cybersecurity. The Director of National Intelligence Jim Clapper, our nation's most senior intelligence advisor to the President, elevated the discussion of cyber space in his recent testimony on the worldwide threat assessment calling it "one of the most challenging [threats] we face.[1]" FBI Director Robert Mueller expressed similar concern, stating "I do believe that the cyber threat will equal or surpass the threat from

[1] Remarks as delivered by James R. Clapper, Director of National Intelligence, Worldwide Threat Assessment to Senate Select Committee on Intelligence, January 31, 2012.

counterterrorism in the foreseeable future.[2]" He continued by equating the challenge posed by today's cyber threat to that of terrorism by stating "the efforts that we put on counterterrorism, the same intensity, the same breaking down [of] stovepipes and the like [has to] be undertaken [with] regard to the cyber threat."

In 2007 and 2008, as Secretary of the Department of Homeland Security during the Bush Administration, I worked closely with the Directors of National Intelligence and the National Security Agency (NSA) to put forward the Comprehensive National Cybersecurity Initiative (CNCI), a now-declassified twelve point strategy to address cybersecurity threats across the civilian and military, government and private domains. Shortly after taking office, President Barack Obama ordered a review of the CNCI, and subsequently strongly reaffirmed the mandate to proceed with a national cyber initiative. President Obama appointed a White House official to coordinate strategy and Congress has taken up possible legislation.

Despite various government efforts, cybersecurity has become an increasingly urgent problem. Over the past year, there have been multiple reports of cyber intrusions across both industry and government, yet each presents different concerns and requires different levels of response. Nevertheless, there is still no comprehensive legislative architecture for cyber defense and security in place today. As I did recently when I signed a joint letter with seven other former executive branch national security officials, I again urge Congress to quickly act and pass comprehensive legislation that will quickly strengthen our nation's cybersecurity.

Looking across a spectrum of areas where legislation can help strengthen our ability to deal with the cyber threat, there are a number about which there should be little controversy. These include:

FISMA Reform – The federal government must continue to apply information security controls for Federal operations commensurate with risk, to ensure federal agencies and departments are consistently monitoring systems, evaluating information security protections and strengthening supply chain security.

Continued Investment in Cyber Education – In order to confront today's cybersecurity threats in both the near and long term, we must have a skilled workforce within government and

[2] Remarks as delivered by Robert Mueller, Director of the Federal Bureau of Investigation, Worldwide Threat Assessment to House Select Committee on Intelligence, February 2, 2012.

throughout the private sector. In addition, we should begin cybersecurity education efforts with the newest Internet users at an early age.

Research and Development – The Federal government needs to continuously support research and development to help us defend against the cyber threat. We need to make investments with innovative technologies that can become quick wins that will help us leap ahead and counter future threat evolutions, as opposed to playing catch up to attacks we have already seen.

But, in my view, in order to really make a difference and confront the growing cyber threat, we need to go further. There are three areas that I believe should be emphasized as a part of any comprehensive cybersecurity legislation: (1) risk-based security standards for our critical infrastructure, (2) information sharing, and (3) liability protections. These areas are reflected in the Lieberman/Collins/Rockefeller/Feinstein "Cyber Security Act of 2012" introduced in the Senate, as well as in a number of House bills and the Administration's own proposal.

Malicious cyber intrusions on privately owned networks may well be carried out – and even mounted – from or through platforms that are privately owned and domestic. These attacks currently steal billions of dollars in intellectual property. Worse yet, crippling of our privately owned transportation networks or our major financial institutions could have a catastrophic national impact, comparable to the effects of a major physical attack.

Some argue that cyber defense and security in our private sector are best left to the market and individual initiative and innovation. While it is true that the private sector has unleashed enormous creativity in developing aspects of our cyber economy, it is far from clear that market incentives will be sufficient to spur adequate investment in cybersecurity. Left to their own devices, few private companies would invest more in securing their cyber assets than the actual value of those assets. Yet in an interconnected and interdependent world, the failure of one part of the network can have devastating collateral and cascading effects across a wide range of physical, economic and social systems. Thus, the market place is likely to fail in allocating the correct amount of investment to manage risk across the breadth of the networks on which our society relies.

Accordingly, responsibility for cyber security should be shared with the government for those privately owned networks and systems which are deemed critical infrastructure based on

interdependence or the essential nature of the services provided. Ownership and control of these networks should remain in private hands, but government is a particularly important partner because it can leverage what former Defense Deputy Secretary William Lynn previously described as "government intelligence capabilities to provide highly specialized active defenses."[3]

In this regards, the approach taken in the Lieberman/Collins/Rockefeller/Feinstein bill to securing private critical infrastructure is important. These proposals do not seek to impose detailed security regimes, but recognize that for identified highly critical infrastructure outcome-based performance standards are necessary. Such performance standards allow private owners the flexibility to innovate in achieving security, but also require in the end that the owners demonstrate that they have attained that appropriate level of security. Similar performance based approaches work well in promoting physical security in our ports, transportation networks, and other key infrastructure.

Will a standards-based mandate impose some cost on owners of essential infrastructure? Probably. But for those responsible owners already investing in adequate security, the marginal cost will be negligible. And for those who are not investing in sufficient security, the price of massive failure – and the collateral damage – will be far more costly.

Beyond setting standards and metrics for securing the most critical infrastructure, Congress must act to promote broader information sharing. In order to better protect our networks from known and emerging threats, both government agencies and private sector companies must have timely information, such as identification of signatures or patterns of behavior that are characteristic of malware. This allows faster detection of ongoing attacks before significant damage is done. We need appropriate guidelines to ensure information can be shared safely between the government and the private sector, so that the government can apply its capability to detect adversaries and convey that information to the private sector. By the same token, private enterprises also gain unique information about the threat as a result of the direct intrusions they are facing daily across multiple sectors. These also need to be shared broadly within the private sector and with the government. All of this must be done in a safe harbor without fear of legal impediments. The "Cybersecurity Act of 2012" includes limitations on liability in order to help facilitate voluntary information sharing for cyber threats. Information shared through appropriate channels cannot be used to trigger regulatory

[3] "Defending a New Domain: The Pentagon's Cyberstrategy," by William J. Lynn III, *Foreign Affairs*, September/October 2010.

enforcement or be the cause for civil or criminal action when such cyber security threat information is shared by a provider of cybersecurity services to a customer, shared with a government entity that manages critical infrastructure or provided to an appropriate cyber security information-sharing exchange.

The legislative efforts currently pending in Congress are important and long-awaited. Cyber attacks are costing us intellectual property and economic growth. One day, they may cost us lives. Congress should not wait to enact remedial legislation.

Thank you again for the opportunity to contribute my personal views on such an important topic that affects both our economic and national security.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Claire McCaskill

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

Question#:	1
Topic:	Section 103
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: How long do you anticipate it will take DHS to implement the procedures that designate covered critical infrastructure under Section 103 and establish performance requirements under Section 104 of the Cybersecurity Act of 2012?

Response: The timeline for implementing a process to designate covered critical infrastructure and establishing risk-based performance requirements, as required by Sections 103 and 104 of S. 2105, will be determined by the Department's engagement with other partners. Establishing new frameworks for critical infrastructure will be a collaborative process that enhances the existing public-private partnership for securing critical networks. Sections 103 and 104 both require extensive engagement with, among others, critical infrastructure owners and operators, the Critical Infrastructure Partnership Advisory Council, Information Sharing and Analysis Organizations, the National Institute of Standards and Technology, the National Security Agency, Sector-Specific Agencies, state and local government, and other Federal agencies to first designate critical infrastructure, and then define appropriate performance outcomes. In order to leverage the expertise of all of these stakeholders, the Department of Homeland Security anticipates that close interaction will be necessary going forward.

Question#:	2
Topic:	Section 104
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Does the bill contain an enforcement mechanism that will be used to ensure compliance with the performance requirements established pursuant to Section 104? If yes, can you explain how you understand such an enforcement mechanism will be utilized and under what circumstances?

Response: The Cybersecurity Act of 2012 authorizes the Department of Homeland Security (DHS) to issue civil penalties to owners of covered critical infrastructure that do not comply with the requirement to demonstrate compliance with the performance requirements established under Section 104, either through a written certification or a third party assessment. The legislation requires that civil penalties be issued in accordance with procedures that would be established through a public rulemaking process, to include consultation with industry. If enacted DHS would manage this program in an open manner with regular collaboration with critical infrastructure owners and would only utilize the enforcement authority when absolutely necessary.

Question#:	3
Topic:	performance
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: Given that cybersecurity threats evolve everyday as the nation's enemies develop new cyber weapons and technology, how will the performance requirements and other regulations authorized by this bill remain effective and keep pace with constantly evolving and sophisticated technological innovation? How often will the performance requirements be updated?

Response: The Department of Homeland Security (DHS) has always maintained the position that private sector innovation is essential to solving the cybersecurity challenge. If enacted, S. 2105 calls for securing critical infrastructure through the development and implementation of high-level performance requirements as opposed to mandating specific technical solutions. This approach would allow each critical infrastructure owner/operator to determine the specific practices that will work on their networks. Moreover, by working with industry to set common performance levels, DHS will encourage the private sector to develop new solutions in those areas. DHS will initiate a process to update the performance requirements (which will be detailed in the public rulemaking) in a timely and technology-neutral, high-level manner.

A key element of DHS cybersecurity strategy is collaboration in research and development efforts, both across DHS components and between DHS and the larger homeland security enterprise. This collaboration is demonstrated in the definition of requirements for cybersecurity capabilities and systems; the Roadmap for Cybersecurity Research (Nov 2009), Strategic Plan for Federal Cybersecurity R&D (Dec 2011), and the National Science and Technology Council's Committee on Technology/Subcommittee on Networking and Information Technology Research and Development Program for Cybersecurity and Information Assurance (Feb 2012) all identify R&D requirements and needed capabilities and a broad collaborative strategy to achieve them. Strong coordination between our operational and R&D teams will enhance the ability to keep pace with both threats and technological innovation.

Question#:	4
Topic:	sectors
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: The bill provides a possible waiver for covered critical infrastructure already governed by sector-specific agency regulations that address the identified risks. Which sectors do you anticipate will receive a waiver from the bill's regulations based on existing sector-specific agency regulations? How will the waiver granting process be implemented and what factors will be used to determine the entities that will receive a waiver?

Response: Section 104 of S. 2105 provides the President with the authority to exempt a covered critical infrastructure entity from the regulatory requirements of the bill if it is determined that an existing regulatory agency has sufficient requirements and enforcement mechanisms to ensure the risks identified by the Department of Homeland Security (DHS) under Section 102 are mitigated.

It would be premature to discuss exempting specific sectors before conducting the sector-by-sector risk assessments and doing a thorough review of existing regulatory capabilities. DHS will establish a clear process in the public rulemaking for the consideration of exemptions.

Question#:	5
Topic:	cyber threats
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Claire McCaskill
Committee:	HOMELAND SECURITY (SENATE)

Question: It has been asserted that certain immunity provisions provided to the private sector in the information sharing provisions of the bill do not go far enough to allow private sector entities to take necessary counter measures against cyber threats. Can you comment on these assertions and provide examples of situations that would result in the denial of immunity from private rights of actions?

Response: The Administration seeks to encourage and incentivize sharing of cybersecurity threat information and taking affirmative steps to protect at-risk information systems.

One of the goals of both the Administration's cybersecurity legislative proposal and the Cybersecurity Act of 2012 is to provide appropriately tailored liability protection and/or immunity to private sector actors. The Administration's proposal provides clear legal authority and corresponding immunity for private sector entities to share cybersecurity information with the Department of Homeland Security (DHS) cybersecurity center and for private sector entities to provide assistance to DHS in carrying out its cybersecurity mission. Section 706 of the Cybersecurity Act of 2012 contains similar provisions and also adds liability protection for private sector monitoring activity in accordance with section 701(1) and (2).

Where civil action is not barred, the Cybersecurity Act of 2012 also provides a good faith defense for private sector individuals and entities engaged in activity permitted under the information sharing provisions of the bill. This good faith defense extends to the deployment of countermeasures under section 701. While such a good faith defense does not bar lawsuits altogether, it does provide a complete defense so long as entities have acted based on a good faith belief that their activities are permitted under the bill.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Ron Johnson

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

Question#:	6
Topic:	costs
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question: A 2011 study by Ohio State University on the costs of homeland security estimated that the private sector has experienced $11B/year in direct homeland security costs. The Cybersecurity Act of 2012 will also have a major impact on the private sector.

a. What is the regulatory burden imposed by this cyber bill?

Response: DHS will, in collaboration with the sector-specific agencies, include a detailed economic analysis in the Notice of Proposed Rulemaking should the legislation become law. The regulations would only apply to a small percentage of the private sector – critical infrastructure that provide life-sustaining services. Additionally, the performance requirements that the covered critical infrastructure would be required to comply with would be based on pre-existing, industry developed practices, standards, and guidelines. Thus, companies that already have robust cybersecurity practices would not be asked to make many changes. It's also important to remember that while the regulations would only touch a small portion of the private sector, the entire private sector relies on the services provided by critical infrastructure. The potential impacts of a cyber incident impeding the delivery of electricity or water to a portion of the United States could be far greater than the cost of the regulations.

Question:
b. What is the total regulatory burden imposed on the private sector by DHS?

Response: DHS imposes regulatory burden on select sectors of the private industry, such as security requirements on the transportation and chemical sectors as well as safety and environmental protection requirements on the maritime sector. For many of these regulations, DHS gets direction from statutory mandates and develops regulations in accordance with those mandates.

Question:

Question#:	6
Topic:	costs
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question:
c. With unemployment currently at 8.3%, how will the Department of Homeland Security ensure that the regulatory regime created under this bill does not inhibit the ability of the private sector to grow, expand, and create jobs?

Response: The regulations would only apply to a small percentage of the private sector – critical infrastructure that provide life-sustaining services. Additionally, the performance requirements that the covered critical infrastructure would be required to comply with would be based on pre-existing, industry developed practices, standards, and guidelines. Thus, companies that already have robust cybersecurity practices would not be asked to make many changes, if any at all. It's also important to remember that while the regulations would only touch a small portion of the private sector, the entire private sector relies on the services provided by critical infrastructure. The Department is committed to managing this program in an open, collaborative manner so that critical infrastructure has an opportunity to contribute to the regulations as they are developed and can provide meaningful input as to how their businesses would be impacted.

However, it's important to remember that the cost of not taking action to better secure our Nation's most critical networks is unacceptably high. Private sector estimates range from $28 billion to $340 billion annual losses from cyber attacks. However, this estimate is based on known financial and intellectual property theft and therefore cannot be fully reflective of unreported incidents. The potential cost of a significant disruption to one or more of our interdependent critical services, such as electricity, communications or transportation, would be much higher. For example, in the cybersecurity scenario the Administration presented to the Senate on March 7, which reviewed the federal response to a 3-day power outage in a large metropolitan area, the impact to GDP was estimated at $1 billion per day, based on an analysis developed by the DHS Office of Infrastructure Protection. However, this scenario was contained to one metro area; losses would be much greater if additional parts of the country were impacted and the duration of the attack extended.

Question:
d. How many Department of Homeland Security promulgated regulations have undergone cost-benefit analysis?

Response: DHS carefully considers the benefits and costs for its regulations during the development and drafting of its regulations. DHS complies with Executive Orders 12866 (Regulatory Planning and Review, October 4, 1993) and 13563 (Improving Regulation and Regulatory Review, January 21, 2011) and adopts only those regulations for which

Question#:	6
Topic:	costs
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

the benefits justify the costs. DHS further considers the impacts of its regulations on small businesses, as required by the Regulatory Flexibility Act.

Question:
i. Of these, how many rules have had benefits exceeding costs? Costs exceeding benefits?

Response: Consistent with the requirements of Executive Orders 12866 and 13563, DHS adopts regulations only upon a reasoned determination that the benefits of the intended regulation justify its costs.

Question:
e. What percentage and number of regulations promulgated by the Department of Homeland Security over the past 3 years are considered to be "major" rules?

Response: Since January 1, 2009, DHS promulgated 4 "major" rules (as defined in section 804 of the Congressional Review Act).

Question:
i. Please provide a list of these rules.

Response: Below is a list of the "major" rules that DHS has promulgated since January 1, 2009.

1. Transportation Security Administration, Air Cargo Screening Final Rule, 76 Fed. Reg. 51,848 (August 18, 2011)
2. U. S. Citizenship and Immigration Services, Fee Schedule Final Rule, 75 Fed. Reg. 58,961 (September 24, 2010)
3. U.S. Customs and Border Protection, Electronic System for Travel Authorization (ESTA): Fee for Use of the System Interim Final Rule, 75 Fed. Reg. 47,701 (August 9, 2010)
4. U.S. Federal Emergency Management Administration, Special Community Disaster Loans Program Final Rule, 75 Fed. Reg. 2,800 (January 19, 2010)

Question:
f. Are there any regulations that you feel the current cost to industry exceed the security benefits achieved?

Response: No. The cost of DHS regulations do not exceed the security benefits achieved from those regulations.

Question#:	7
Topic:	CBO
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question: Billions of dollars have been spent on cyber security over the past few years by the Department of Homeland Security, the Department of Defense, and other federal agencies. The 2010 cyber bill introduced by Senators Collins and Lieberman was estimated by the Congressional Budget Office (CBO) to cost at least $1.5B.

a. Understanding our cyber system will never be 100% perfect, how much money will it take to adequately "secure" the cyber domain?

b. How do we ensure that every dollar spent is the most effective use of taxpayer dollars?

Response: The President's Budget Request provides the Department of Homeland Security with resources to continue driving cyber risk reduction and risk management. The Department's deliberative budget process is designed to allocate resources across programs in a strategic manner that addresses the entirety of the cyber domain and that supports the greatest results for taxpayer dollars spent.

In December 2011, the Department published its *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*, which proposes a path forward to achieve the cybersecurity goals outlined in the Quadrennial Homeland Security Review and will drive the development of future budgets in a prioritized, comprehensive manner.

Question#:	8
Topic:	companies
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Ron Johnson
Committee:	HOMELAND SECURITY (SENATE)

Question: In the recent cybersecurity hearing before this Committee, Senator Johnson asked whether "... you have a list of private sector companies that would have to comply with this [bill] that are in favor of it?" In response, you stated "there are a number, and I think they have been in contact with the Committee but we can get that for you."

Please identify these companies. If a company has written a letter of support for the bill, please attach the letter.

Response: The private sector outreach on S. 2105 was led by the sponsors of the bill, Senators Lieberman, Collins, Rockefeller and Feinstein. Letters of support can be found on the Senate Homeland Security and Governmental Affairs Committee's website, which is updated regularly as more firms express their support, can be found at www.hsgac.senate.gov/issues/cybersecurity. More than 20 private sector companies and organizations have expressed their support as of this writing. However, I appreciate the opportunity to clarify my response to your request to specifically name companies 'that would have to comply with this [bill]." Identifying individual companies that will be covered by the performance requirements would be premature and undermine the open, collaborative designation process described above.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Thomas R. Carper

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

Question#:	9
Topic:	cyber attacks
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: In addition to federal cybersecurity efforts, we must take strong steps to better prepare state and local officials for cyber attacks. As you may know, my home state of Delaware has devoted significant time and resources to enhancing its cyber education and awareness. In fact, Delaware has a proven track record of using real-time exercises, including several DHS "Cyber Storm" exercises, to prepare and train local officials for cyber incidents. I understand the Cybersecurity Act of 2012 calls for an education campaign to increase the cyber awareness of state and local governments, but as grant budgets at your department get smaller and state budgets shrink as well, how will you continue the hands-on training that has helped my State become a leader in cybersecurity? Are there any current cyber programs that Congress should be looking at as models for outreach and training?

Response: The Department continues to work with state and local governments through a number of outreach, training, and exercise programs. The Cyber Exercise Program (CEP) works with Federal, state, local, international, and private sector partners to conduct regional and sector-specific exercises designed to develop and improve the capabilities of DHS and its infrastructure partners. Such exercises aid in prevention and recovery from the Nation's critical infrastructure cyber breaching incidents. The National Cyber Security Division plans, coordinates, and conducts cyber exercises to develop, evaluate, improve, and refine the capabilities of state and local partners. This includes the Cyber Storm exercises, which provide state government network security professionals greater technical security skills and practical experience with implementing the principles of effective cyber defense. Cyber Storm IV will take place over a period of roughly 10 months, which began on January 2012 and will conclude in October 2012. The exercise is segregated into two primary focus groups; the Cyber Storm IV- State Cyber Coordination Exercise, which includes a total of nine states, and the Cyber Storm IV- Individual State Exercises, with a current total of four states. Additionally, the Cyber Exercise Program, alongside the Federal Emergency Management Agency's National Continuity Program, sponsors a joint workshop titled Resilient Accord which focuses on

Question#:	9
Topic:	cyber attacks
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

cybersecurity considerations for emergency planners. The on-going series is delivered throughout the nation and is focused on educating State and local officials about cyber risk and mitigation strategies.

The Department also engages in a number of efforts to foster cybersecurity awareness. Most prominently, the Office of Cybersecurity and Communications (CS&C) leads the *Stop.Think.Connect.* Campaign, a year-round cybersecurity awareness and public service campaign aimed at increasing Americans' understanding of cyber threats and empowering them to be safer and more secure online. *Stop.Think.Connect.* is a cornerstone of the National Initiative for Cybersecurity Education (NICE), which was created in response to the priorities expressed in the President's Cyberspace Policy Review. Federal agencies and state, local, tribal, and territorial governments have the opportunity to become members of the *Stop.Think.Connect.* coalition, collaborate with the Campaign on outreach efforts to target audiences, and access Campaign materials, templates, and other resources to help promote cybersecurity awareness. In addition, CS&C promotes free resources dedicated to cybersecurity education and training. Links to these resources are available on the *Stop.Think.Connect.* website (www.dhs.gov/stopthinkconnect) and include the National Cyber Security Alliance's Stay Safe Online program and the Federal Trade Commission's Onguard Online.

The Department also developed the Integrated Cybersecurity Education Communities (ICEC) project to equip the Nation's high school teachers with the tools to integrate cybersecurity principles into their classrooms, including cyber-integrated curricula. The intent of the project, which focuses on U.S. high school teachers and their students, is to motivate academically capable students into pursuing cybersecurity studies and careers. This project will be piloted this year and, if successful and subject to available funding, will be phased in to multiple communities across the U.S. DHS envisions that teachers who participate will affect approximately 1.7 million students over ten years if the model is rolled out to all 50 states.

The Department is also leading an effort, through the Science and Technology Directorate and NICE, to utilize cyber security competitions more effectively. The goal is to not only motivate the future workforce, but also provide the means to identify and guide individuals through a curriculum tailored to specific needs of the individual and the nation. The three pronged approach employs a matrix of cyber security competitions, an assessment framework of these competitions and the competing students, and a social network style community for students, competition organizers and potential employers to interact with each other and track progress toward their common goals.

An additional component of the cyber security competitions program is to introduce new technologies to the future workforce. DHS is working with the organizers of the National Collegiate Cyber Defense Challenge to include emerging defense technologies into the competition architecture to familiarize the students and eventually drive the adoption of the technologies into the national infrastructure as the students are employed.

Question#:	10
Topic:	regulations
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Question: From what I understand, the Cybersecurity Act of 2012 defers to existing cyber regulations or industry-led standards that are effectively stopping cyber threats, before requiring any new Homeland Security regulations. This is important for areas like the banking and financial sector that have a long history of implementing cybersecurity measures. Do you believe complying with the Cybersecurity Act of 2012 would undermine the security measures that many sectors, like the banking industry, are already taking? I recognize that the bill calls for significant consultation throughout the regulatory process, but can you discuss how the Department would work to acquire the necessary expertise to make cyber determinations about all the different critical infrastructure sectors?

Response: The regulations would only apply to a small percentage of the private sector – critical infrastructure that provide life-sustaining services. Additionally, the performance requirements that the covered critical infrastructure would be required to comply with would be based on pre-existing, industry developed practices, standards, and guidelines. Thus, companies that already have robust cybersecurity practices would not be asked to make many changes. It's also important to remember that while the regulations would only touch a small portion of the private sector, the entire private sector relies on the services provided by critical infrastructure.

Section 104 of the Cybersecurity Act of 2012 specifically requires the Secretary of Homeland Security to establish a process for reviewing existing cybersecurity performance requirements to determine if existing regulations appropriately address identified cyber risks. If there are adequate regulations already in place, the President may exempt certain covered critical infrastructure from the requirements. It is our goal to build upon the good work that has been done in certain sectors and assist in filling the gaps as needed. We believe that the cybersecurity requirements of the Cybersecurity Act of 2012 will not impede the current security measures taken by many of the sectors, including the banking industry.

The Department has a strong and proven track record assisting the private sector, critical infrastructure, and other Federal partners with successfully identifying and mitigating a range of cyber risks. For example, last year the DHS U.S. Computer Emergency Readiness Team (US-CERT) received more than 100,000 incident reports, and released more than 5,000 actionable cybersecurity alerts and information products.

Question#:	10
Topic:	regulations
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Thomas R. Carper
Committee:	HOMELAND SECURITY (SENATE)

Should the legislation pass, we will immediately draw upon resources from across the Department and the Executive Branch to implement the requirements for critical infrastructure cybersecurity. As part of our current responsibilities, the Department is already working closely with critical infrastructure owners to understand their cybersecurity preparedness to deal with a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Our cyber experts, our infrastructure protection experts, and regulatory experts from across the Department and in the sector-specific agencies form a broad basis from which to take up the additional responsibilities in the bill and to minimize the burden on the private sector while promoting better security practices across the board.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Tom Coburn

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

Question#:	11
Topic:	US-CERT
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: The DHS Inspector General has found that the network of DHS's US-Computer Emergency Readiness Team (US-CERT) to be vulnerable to computer intrusions. Why should we trust DHS to oversee federal and civilian cyber security when DHS apparently cannot protect its own network? What has been done since the 2010 audit to fix the problem?

Response: The Department of Homeland Security (DHS) takes its cybersecurity and Federal Information Security Management Act responsibilities very seriously. The National Cyber Security Division (NCSD) took immediate corrective actions in connection with the OIG's findings. In fact, at the time of the Office of Inspector General (OIG) audit, NCSD was already in the process of implementing solutions to avoid the problems noted in the OIG's report. As a result, NCSD was able to submit documentation to the OIG before the final report was issued in August 2010 that demonstrated corrective actions and support for the closure of recommendations. For example, NCSD demonstrated that:

- As of June 30, 2010, NCSD had deployed a software management solution that automatically deploys security patches to mitigate future vulnerabilities;
- As of July 12, 2010, the noted vulnerabilities had been remediated; and
- As of August 27, 2010, NCSD had improved its internal process to track discovered vulnerabilities until remediated, including a revised, comprehensive "Network Scanning" Standard Operating Procedure.

Further, NCSD provided the OIG with documentation as evidence that it had formalized its security personnel training program. NCSD also demonstrated that it uses the Defense Information System Agency Security Technical Implementation Guide as an automated tool for configuration management, not as a replacement for DHS baseline configuration

Question#:	11
Topic:	US-CERT
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

settings, which the OIG alleged, but instead to supplement the baseline and to achieve a more robust and secure posture.

It should also be noted that the OIG found that NCSD had taken a number positive steps such as implementing sufficient physical security and logical access controls over the cybersecurity program systems used to collect, process, and disseminate cyber threat and warning information to the public and private sectors.

The OIG closed a number of its recommendations within several months of issuing its report and it communicated in a September 15, 2011 memorandum that all recommendations had been implemented and closed as of August 31, 2011.

Question#:	12
Topic:	contracts
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Are you confident that the cyber security firms that DHS contracts with are not being penetrated by cyber attacks by foreign actors? What actions has DHS taken to ensure that the contractors it works with are not being compromised by cyber attacks?

Response: To help reduce the risks posed to DHS information and infrastructure, DHS maintains policies governing the types of government information that can be stored on non-government controlled networks, works with critical infrastructure owners and operators to mitigate reported incidents upon their request, vets contractors and their employees who propose to work on DHS matters, and incorporates cyber security standards into contracts with companies that host or manage DHS information systems.

As part of the Personnel Security and Suitability Program under the Office of the Chief Security Officer, all DHS contractors are vetted to ensure they are fit to work on behalf of DHS. The vetting process for this program includes law enforcement checks (FBI databases) as well as other investigative checks, focusing on personnel and their trustworthiness.

The DHS vetting process specific to contractor companies, their database systems, and employees is detailed in the DHS Information Systems Security Policy 4300A and the information security clauses from the Homeland Security Acquisition Regulations (HSAR) that are an adjunct to the Federal Acquisition Regulations (FAR). The HSAR contract clauses lay out in specific detail the requirements for system and personnel vetting, system authorization, submission of security plans, and the requirement to follow the current version of the DHS Security Publication 4300A. DHS ensures the HSAR clauses are included in all contracts by reviewing acquisitions in excess of $2.5 million, consistent with DHS HQ Management Directives 0007.1 and AD 102.02, and with Components' specific processes for smaller contracts. These include requirements that contractor personnel must obtain suitability through the DHS Suitability process which is detailed in the HSAR Clause 3052.204-71 entitled, "Contractor Employee Access," which includes a review of numerous National Agency records including from the U.S. Department of Justice.

The HSAR Clause 3052.204-70 entitled, "Security Requirements for Unclassified Information Technology Resources," details how contractors must handle sensitive but unclassified information in compliance with MD 11042.1 entitled, "Safeguarding Sensitive But Unclassified (For Official Use only) Information." The clause requires the contractor, within 45 days of contract award, to provide a security plan that details how

Question#:	12
Topic:	contracts
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

the contractor applies various security controls (from DHS Information Security Policy and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 "Recommended Security Controls for Federal Information Systems and Organization") to secure the information and/or information system. This clause also requires the contractor to comply with MD 4300.1, entitled, "Information Technology Systems Security," and the DHS Sensitive Systems Handbook which prescribes the policies and procedures on security for information technology resources. Compliance with these policies and procedures, any replacement publications, or any other current or future DHS policies and procedures covering contractors specifically is required in all contracts that require access to facilities, IT resources, or sensitive information.

The complete 4300A and HSAAR Security Clauses are attached.

3004.4 Safeguarding Classified and Sensitive Information within Industry.
3004.470 Security requirements for access to unclassified facilities, Information Technology resources, and sensitive information.
3004.470-1 Scope.
This section implements DHS's policies for assuring the security of unclassified facilities, Information Technology (IT) resources, and sensitive information during the acquisition process and contract performance.
3004.470-2 Policy.
(a) DHS's policies and procedures on contractor personnel security requirements are set forth in various management directives (MDs). MD 11042.1, Safeguarding Sensitive But Unclassified (For Official Use only) Information describes how contractors must handle sensitive but unclassified information. MD 4300.1, entitled Information Technology Systems Security, and the DHS Sensitive Systems Handbook, prescribe the policies and procedures on security for Information Technology resources. Compliance with these policies and procedures, any replacement publications, or any other current or future
4-1 06-01-2006 HSAR
DHS policies and procedures covering contractors specifically is required in all contracts that require access to facilities, IT resources or sensitive information.
(b) The contractor must not use or redistribute any DHS information processed, stored, or transmitted by the contractor except as specified in the contract.
3004.470-3 Contract clauses.
(a) Contracting officers shall insert a clause substantially the same as the clause at (HSAR) 48 CFR 3052.204-70, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts that require submission of an IT Security Plan.
(b) Contracting officers shall insert the basic clause at (HSAR) 48 CFR 3052.204-71, Contractor Employee Access, in solicitations and contracts when contractor employees require recurring access to Government facilities or access to sensitive information. Contracting Officers shall insert the basic clause with its Alternate I for acquisitions requiring contractor access to IT resources. For acquisitions in which the contractor will not have access to IT resources, but the Department has determined contractor employee access to sensitive information or Government facilities must be limited to U.S. citizens and lawful permanent residents, the contracting officer shall insert the clause with its Alternate II. Neither the basic clause nor its alternates shall be used unless contractor employees will require recurring access to Government facilities or access to sensitive information. Neither the basic clause nor its alternates should ordinarily be used in contracts with educational institutions.
Subpart 3004.8 Government Contract Files
3004.804 Closeout of contract files.
3004.804-1 Closeout by the office administering the contract.
(b) The quick closeout procedures under (FAR) 48 CFR 42.708 may be used for the settlement of indirect costs under contracts when the estimated amount (excluding any fixed fee) of the contract is $3 million or less if determined appropriate by the contracting officer.
3004.804-5 Procedures for closing out contract files.
3004.804-570 Supporting closeout documents.
(a) When applicable and prior to contract closure, the contracting officer shall obtain the listed DHS and Department of Defense (DOD) forms from the contractor for closeout.
(1) DHS Form 0700-03, Contractor's Release (e.g., see (FAR) 48 CFR 52.216-7);

(2) DHS Form 0700-02, Contractor's Assignment of Refunds, Rebates, Credits and Other Amounts (e.g., see (FAR) 48 CFR 52.216-7);
(3) DHS Form 0700-01, Cumulative Claim and Reconciliation Statement (e.g., see (FAR) 48 CFR 4.804-5(a)(13); and
(4) DD Form 882, Report of Inventions and Subcontracts (e.g., see (FAR) 48 CFR 52.227-14).
(b) The forms listed in this section (see (HSAR) 48 CFR Part 3053) are used primarily for the closeout of cost-reimbursement, time-and-materials, and labor-hour contracts. The forms may also be used for closeout of other contract types to protect the Government's interest.

3052.204-70 Security requirements for unclassified information--technology resources.

As prescribed in (HSAR) 48 CFR 3004.470-4 Contract clauses, and (HSAR) 48 CFR 3037.110-70 (a) and (b), insert a clause substantially the same as follows:

Security Requirements for Unclassified Information Technology Resources (Dec. 2003)

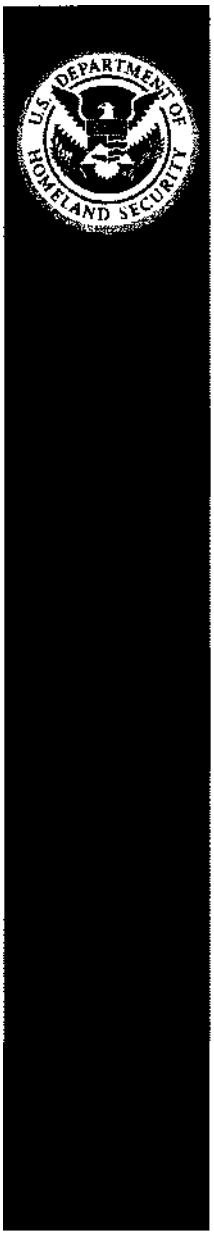
(a) The Contractor shall be responsible for Information Technology (IT) security for all systems connected to a DHS network or operated by the Contractor for DHS, regardless of location. This clause applies to all or any part of the contract that includes information technology resources or services for which the Contractor must have physical or electronic access to sensitive information contained in DHS unclassified systems that directly support the agency's mission. The security requirements include, but are not limited to, how the Department of Homeland Security's sensitive information is to be handled and protected at the Contractor's site, (including any information stored, processed, or transmitted using the Contractor's computer systems), the background investigation and/or clearances required, and the facility security required. This requirement includes information technology, hardware, software, and the management, operation, maintenance, programming, and system administration of computer systems, networks, and telecommunications systems. Examples of tasks that require security provisions include--
(1) Acquisition, transmission or analysis of data owned by DHS with significant replacement cost should the contractor's copy be corrupted; and
(2) Access to DHS networks or computers at a level beyond that granted the general public, (e.g. such as bypassing a firewall).
(b) At the expiration of the contract, the contractor shall return all sensitive DHS information and IT resources provided to the contractor during the contract, and a certification that all DHS information has been purged from any contractor-owned system used to process DHS information. Organizational elements shall conduct reviews to ensure that the security requirements in the contract are implemented and enforced.
(c) The Contractor shall provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources

that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractor's IT Security Plan shall be compliant with Federal laws that include, but are not limited to, the Computer Security Act of 1987 (40 U.S.C. 1441 et seq.), and the Government Information Security Reform Act of 2000, and the Federal Information Security Management Act of 2002. The plan shall meet IT security requirements in accordance with Federal policies and procedures that include, but are not limited to OMB Circular A-130, Management of Federal Information Resources, Appendix III, and Security of Federal Automated Information Resources;

(d) Within----days after contract award, the contractor shall submit for approval an IT Security Plan. This plan shall be consistent with and further detail the approach contained in the offeror's proposal or quote that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will be according to the criteria of the Homeland Security Information Technology Security program Publication, DHS MD 4300.Pub., Volume I, Policy Guide, Part A, Sensitive Systems, which is available from the Contracting Officer upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The contractor shall comply with the approved accreditation documentation.

(End of clause)



DHS Sensitive Systems Policy Directive 4300A

Version 9.0.2

March 19, 2012

This Policy implements
DHS Management Directive 140-01,
Information Technology System Security, July 31, 2007

DEPARTMENT OF HOMELAND SECURITY

FOREWORD

The Department of Homeland Security (DHS) 4300 series of information security policies are the official documents that create and publish Departmental standards and guidelines in accordance with DHS Management Directive 140-01 *Information Technology System Security.*

Comments concerning DHS Information Security publications are welcomed and should be submitted to the DHS Director for Information Systems Security Policy at INFOSEC@dhs.gov or addressed to:

DHS Director of Information Security Policy
OCIO CISO Stop 0182
Department of Homeland Security
245 Murray Lane SW
Washington, DC 20528-0182

/S/

Emery Csulak
Chief Information Security Officer, Acting
Department of Homeland Security

TABLE OF CONTENTS

1.0 INTRODUCTION

This document articulates the Department of Homeland Security (DHS) Information Security Program policies for sensitive systems. Procedures for implementing these policies are outlined in a companion publication, DHS 4300A *Sensitive Systems Handbook*. The Handbook serves as a foundation on which Components are to develop and implement their own information security programs. The Baseline Security Requirements (BLSR) included in the Handbook must be addressed when developing and maintaining information security documents.

1.1 Information Security Program

The DHS Information Security Program provides a baseline of policies, standards, and guidelines for DHS Components. This Policy Directive provides direction to managers and senior executives for managing and protecting sensitive systems. It also defines policies relating to management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, authenticity, and nonrepudiation in DHS information system infrastructure and operations. The policy elements expressed in this Policy Directive are designed to be broad in scope. Implementation information can often be found in specific National Institute of Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, *Recommended Security Controls for Federal Systems and Organizations*.

The policies and direction contained in this document apply to all DHS Components. Information security policies and implementation procedures for National Security Systems are covered in the separate publication set, *DHS National Security Systems Policy Directive 4300B* and *DHS 4300B National Security Systems Handbook*, which are available on the DHS Chief Information Security Officer (CISO) website.

Policy elements are effective when issued. Any policy elements that have not been implemented within ninety (90) days shall be considered a weakness and either a system or program Plan of Action and Milestones (POA&M) must be generated by the Component for the identified weaknesses. When this Policy Directive is changed, the CISO will ensure that appropriate changes in DHS Security Compliance tools, Risk Management System (RMS), and Trusted Agent FISMA[1] (TAF); tool changes are made available to the Department within forty-five (45) days of the changes.

1.2 Authorities

The following are authoritative references for the DHS Sensitive Information Security Program. Additional references are located in Appendix C to this Policy Directive.

- *Title III, E-Government Act of 2002 Federal Information Security Management Act of 2002*, 44 U.S.C. 3541
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*

[1] *FISMA: Federal Information Security Management Act, 44 U.S.C 3541*

- DHS Management Directive (MD) 140-01, *Information Technology Security Services*
- NIST Federal Information Processing Standards (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*

1.3 Policy Overview

DHS information security policies define the security management structure and foundation needed to measure progress and compliance. Policies in this document are organized in three sections:

- **Management Controls** – These controls focus on managing both system information security controls and system risk. These controls consist of risk mitigation techniques normally used by management.
- **Operational Controls** – These controls focus on mechanisms primarily implemented and executed by people. Operational controls are designed to improve the security of a particular system or group of systems and often rely on management and technical controls.
- **Technical Controls** – These controls focus on security controls executed by information systems. Technical controls provide automated protection from unauthorized access or misuse; facilitate detection of security violations; and support security requirements for applications and data.

1.4 Definitions

The definitions in this section apply to the policies and procedures discussed in this document. Other definitions may be found in the *National Information Assurance (IA) Glossary*, as well as *Privacy Incident Handling Guidance* and the *Privacy Compliance* documentation issued by the DHS Privacy Office.

1.4.1 Sensitive Information

Sensitive information is information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal programs or other programs or operations essential to the national interest. Examples of sensitive information include personal data such as Social Security numbers; trade secrets; system vulnerability information; pre-solicitation procurement documents, such as statements of work; and information pertaining to law enforcement investigative methods; similarly, detailed reports related to computer security deficiencies in internal controls are also sensitive information because of the potential damage that could be caused by the misuse of this information. System vulnerability information about a financial system shall be considered Sensitive Financial Information. All sensitive information must be protected from loss, misuse, modification, and unauthorized access.

1.4.2 Public Information

This type of information can be disclosed to the public without restriction but requires protection against erroneous manipulation or alteration (e.g., public websites).

1.4.3 National Security Information

Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, or any predecessor order, to require protection against unauthorized disclosure.

1.4.4 Classified National Security Information

Information that has been determined, pursuant to Executive Order 13526, *Classified National Security Information*, to require protection against unauthorized disclosure and is marked to indicate its classified status.

1.4.5 National Intelligence Information

The following definition is provided in the *Intelligence Reform and Terrorism Prevention Act of 2004*, 118 Stat. 3638:

> "The terms 'national intelligence' and 'intelligence related to national security' refer to all intelligence, regardless of the source from which derived and including information gathered within or outside the United States, that – "(A) pertains, as determined consistent with any guidance issued by the President, to more than one United States Government agency; and "(B) that involves – (i) threats to the United States, its people, property, or interests; (ii) the development, proliferation, or use of weapons of mass destruction; or (iii) any other matter bearing on United States national or homeland security."

1.4.6 Foreign Intelligence Information

This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence except for information on international terrorist activities.

1.4.7 Information Technology

Division E of Public Law 104-106, the *Information Technology Management Reform Act of* 1996 40 U.S.C. 1401 et seq., commonly referred to as the Clinger-Cohen Actof 1996, defines Information Technology (IT) as

> "any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an Executive agency."

For purposes of the preceding definition, "equipment" refers to that used by any DHS Component or contractor, if the contractor requires the use of such equipment in the performance of a service or the furnishing of a product in support of DHS.

The term *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

The term *information system* as used in this policy document, is equivalent to the term *IT system*.

1.4.8 DHS System

A DHS system is any information system that transmits, stores, or processes data or information and is (1) owned, leased, or operated by any DHS Component; (2) operated by a contractor on behalf of DHS; or (3) operated by another Federal, state, or local Government agency on behalf of DHS. DHS systems include *general support systems* and *major applications*.

1.4.8.1 General Support System

A *general support system* (GSS) is an interconnected set of information resources that share common functionality and are under the same direct management control. A GSS normally includes hardware, software, information, applications, communications, data and users. Examples of GSS include local area networks (LAN), including smart terminals that support a branch office, Department-wide backbones, communications networks, and Departmental data processing centers including their operating systems and utilities.

Note: Security for GSSs in use at DHS Headquarters shall be under the oversight of the DHS Office of the Chief Information Officer (OCIO), with support from the DHS Enterprise Operations Center (EOC). All other GSSs shall be under the direct oversight of respective Component CISOs, with support from the Component's Security Operations Center (SOC). Every GSS must have an Information Systems Security Officer (ISSO) assigned.

1.4.8.2 Major Application

A *major application* (MA) is an automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.[2]" [Note: All Federal applications require some level of protection.] Certain applications, because of the information they contain, however, require special management oversight and should be treated as MAs. An MA is distinguishable from a GSS by the fact that it is a discrete application, whereas a GSS may support multiple applications. Each MA must be under the direct oversight of a Component CISO or Information System Security Manager (ISSM), and must have an ISSO assigned.

1.4.9 Component

A DHS *Component* is any organization which reports directly to the Office of the Secretary (including the Secretary, the Deputy Secretary, the Chief of Staff, the Counselors, and their respective staff, when approved as such by the secretary.

1.4.10 Trust Zone

A *Trust Zone* consists of any combination of people, information resources, data systems, and networks that are subject to a shared security policy (a set of rules governing access to data and services). For example, a Trust Zone may be set up between different network segments that require specific usage policies based on information processed, such as law enforcement information.

---

[2] OMB Circular A-130

1.4.11 Continuity of Operations

Internal organizational efforts to ensure that a viable capability exists to continue essential functions across a wide range of potential emergencies, through plans and procedures that:

- Delineate essential functions and supporting information systems
- Specify succession to office and the emergency delegation of authority
- Provide for the safekeeping of vital records and databases
- Identify alternate operating facilities
- Provide for interoperable communications
- Validate the capability through tests, training, and exercises

1.4.12 Continuity of Operations Plan

A plan that provides for the continuity of essential functions of an organization in the event that an emergency prevents occupancy of its primary facility. It provides the organization with an operational framework for continuing its essential functions when normal operations are disrupted or otherwise cannot be conducted from its primary facility.

1.4.13 Essential Functions

Essential Functions are those that enable Executive Branch agencies to provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain industrial capability andthe national economy base during an emergency.

1.4.14 Vital Records

Vital records are Electronic and hardcopy documents, references, , databases, and information systems needed to support essential functions under the full spectrum of emergencies. Categories of vital records may include:

- *Emergency operating records* – emergency plans and directive(s); orders of succession; delegations of authority; staffing assignments; selected program records needed to continue the most critical agency operations; and related policy or procedural records.
- *Legal and financial rights records* – records that protect the legal and financial rights of the Government and of the individuals directly affected by its activities. Examples include accounts receivable records, social security records, payroll records, retirement records, and insurance records. These records were formerly defined as "rights-and-interests" records.
- *Records used to perform national security preparedness functions and activities* in accordance with Executive Order (EO).

1.4.15 Operational Data

Operational data is information used in the execution of any DHS mission.

1.4.16 Federal Information Security Management Act

FISMA requires each agency to develop, document, and implement an agency-wide information security program that will provide a high-level of security for the information and information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Statutory requirements include:

(1) Periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency.

(2) Policies and procedures that:

a. Are based on the risk assessments required by paragraph (1) above

b. Cost-effectively reduce information security risks to an acceptable level

c. Ensure that information security is addressed throughout the life cycle of each agency information system

d. Ensure compliance with

i. Other applicable Federal policies and procedures as may be prescribed by OMB and NIST Minimally acceptable system configuration requirements, as determined by the agency

ii. Any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President

(3) Subordinate plans for providing adequate information security for networks, facilities, and information systems, as appropriate;

(4) Security awareness training to inform personnel, including contractors, others working on behalf of DHS, and others who use information systems supporting operations and assets of the Department. Such training shall convey knowledge of

a. Information security risks associated with their activities

b. Their responsibility to comply with agency policies and procedures designed to reduce these risks

(5) Periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually. This testing:

a. Shall include testing of management, operational, and technical controls of every information system identified in the Department's inventory

b. May include testing relied on by the Office of Inspector General (OIG)

(6) A process for planning, implementing, evaluating, and documenting remedial actions to address any deficiencies in the Department's information security policies, procedures, and practices

(7) Procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines published by the United States Computer Emergency Readiness Team (US-CERT)

a. Mitigating risks associated with incidents before substantial damage is done

b. Notifying and consulting with US-CERT

c. Notifying and consulting with:

i. Law enforcement agencies and relevant OIG

ii. An office designated by the President for any incident involving a national security system

iii. Other agency or offices, as required

(8) Plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the Department

FISMA requires that the Chief Information Officer (CIO) designate a senior agency information security official who shall develop and maintain a Department-wide information security program. The designee's responsibilities include:

- Developing and maintaining information security policies, procedures, and control techniques that address all applicable requirements
- Training and overseeing personnel with significant information security responsibilities
- Assisting senior Department officials with respect to their responsibilities under the statute
- Ensuring that the Department has sufficient trained personnel to ensure the Department's compliance with the statute and related policies, procedures, standards, and guidelines
- Ensuring that the Department CIO, in coordination with other senior Department officials, reports annually to the Secretary on the effectiveness of the Department's information security program, including the progress of remedial actions

1.4.17 Personally Identifiable Information

Personally Identifiable Information (PII) is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether the individual is a U.S. citizen, lawful permanent resident, a visitor to the U.S., or a Department employee or contractor.

1.4.18 Sensitive Personally Identifiable Information

Sensitive PII is PII which if lost, compromised, or disclosed without authorization could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, Alien Registration Numbers (A-Number), criminal history information, and medical information. Sensitive PII requires more stringent handling guidelines because of the greater sensitivity of the information.

1.4.19 Privacy Sensitive System

A *Privacy Sensitive System* is any system that collects, uses, disseminates, or maintains PII or Sensitive PII.

1.4.20 Strong Authentication

Strong authentication is a layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.

1.4.21 Two-Factor Authentication

Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). *Single-factor authentication* uses only one of the three forms of authentication, while *two-factor authentication* uses any two of the three forms. *Three-factor authentication* uses all three forms.

1.5 Waivers and Exceptions

1.5.1 Waivers

Components may request waivers to, or exceptions from, any portion of this Policy Directive for up to six (6) months at any time they are unable to fully comply with a Policy Directive requirement. Waiver requests are routed through the Component's ISSO for the system, to the Component's CISO or ISSM, and then to the DHS CISO. All submitters shall coordinate with the Authorizing Official (AO) prior to submission. If a material weakness is reported in an audit report, and the weakness is not scheduled for remediation within twelve (12) months, the Component must submit a waiver request to the DHS CISO. If the material weakness is in a financial system, the Component Chief Financial Officer (CFO) must also approve the waiver request before sending to the DHS CISO.

In all cases, waivers shall be requested for an appropriate period based on a reasonable remediation strategy.

1.5.2 Exceptions

Components may request an exception whenever unable to bring a system control weakness into compliance or when a weakness requires a permanent exception to DHS policy. Exceptions are usually limited to systems that are unable to comply due to detrimental impact on mission, excessive costs, or, for non-essential systems, clearly documented end of platform life within eighteen (18) months, or for commercial-off-the-shelf (COTS) products that cannot be configured to support the control requirement. Exception requests are routed through the Component CISO/ISSM, to the DHS CISO. All submitters shall coordinate with the AO prior to submission.

The risk that results from the exception also must be approved and accepted by the AO and by the Component CFO if the system is a financial or mixed financial system.

1.5.3 Waiver or Exception Requests

The Waivers and Exceptions Request Form found in Attachment B of the *DHS 4300A Sensitive Systems Handbook* shall be used.

Component ISSOs, audit liaisons, and others may develop the waiver or exception request, but the System Owner shall submit the request through the Component's CISO/ISSM.

Waiver requests shall include documentation of mission impact as operational justification; mission impact, risk acceptance; risk mitigation measures; and a POA&M for bringing the system procedures or control weakness into compliance.

Exception requests shall include the operational justification (document mission impact), as well as efforts to mitigate the risk based to include descriptions of counter measures or compensating controls currently in place.

Any waiver or exception requests for CFO-Designated Systems must be submitted to and approved by the Component's CFO prior to the DHS CFO's submission to the DHS CISO. Any waiver or exception requests for Privacy Sensitive Systems must be submitted to and approved by the Component's Privacy Officer or senior Privacy Point of Contact (PPOC) prior to being submitted to the DHS CISO.

All approved waiver and exception requests must be directed through the Component's CISO/ISSM who will in turn direct them to the DHS CISO.

Policy ID	DHS Policy Statements	Relevant Controls
1.5.3.a	This Policy Directive and the DHS 4300A Sensitive Systems Handbook apply to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data unless an approved waiver or exception has been granted. This includes prototypes, telecommunications systems, and all systems in all phases of the Systems Engineering Life Cycle (SELC).	---
1.5.3.b	Systems without an Authority to Operate (ATO) when this policy is issued shall comply with all of its policy statements or obtain appropriate waivers and/or exceptions. Systems with an ATO shall comply within 90 days of the date of this Policy is issued or obtain appropriate waivers and/or exceptions. (A new ATO is only required for significant changes.)	PL-1
1.5.3.c	Each waiver or exception request shall include the system name, and system TAF Inventory ID, operational justification, and risk mitigation.	CM-3
1.5.3.d	Components shall request a waiver whenever they are *temporarily* unable to comply fully with any portion of this policy.	CA-2
1.5.3.e	All waiver requests shall identify the POA&M for bringing the system or program into compliance.	CA-5, PM-4

Policy ID	DHS Policy Statements	Relevant Controls
1.5.3.f	The Component CISO/ISSM shall approve all waiver requests prior to submitting them to the DHS CISO.	CA-6
1.5.3.g	Waiver requests submitted without sufficient information shall be returned for clarification prior to making a decision.	CA-6
1.5.3.h	A waiver shall normally be issued for six (6) months or less. The DHS CISO may issue waivers for longer than six (6) months in exceptional situations. Waivers may be renewed by following the same process as in the initial request.	CA-2
1.5.3.i	The Head of the Component shall approve any waiver request that results in a total waiver time exceeding twelve (12) months before sending the request to the DHS CISO. The waiver shall also be reported as a material weakness in the Component's FISMA report.	---
1.5.3.j	Components shall request an exception whenever they are permanently unable to fully comply with any portion of this policy.	CA-2
1.5.3.k	All approved waivers shall be reported in the Component's FISMA report.	CA-6
1.5.3.l	The DHS CFO shall approve all requests for waivers and exceptions for financial systems prior to their submission to the DHS CISO.	CA-6
1.5.3.m	The Component's Privacy Officer or Senior PPOC shall approve all requests for waivers and exceptions for Privacy Sensitive Systems prior to their submission to the DHS CISO.	---

1.5.4 Requests for Exception to U.S. Citizenship Requirement

Special procedures apply for exception to the requirement that persons accessing DHS systems be U.S. citizens. Under normal circumstances, only U.S. citizens are allowed access to DHS systems and networks; but there is a need at times to grant access to foreign nationals. Access for foreign nationals is normally a long-term commitment, and exceptions to pertinent policies are treated separately from standard exceptions and waivers. The approval chain for an exception to the U.S. citizenship requirement flows through the Component Head, the Office of Security, and the CIO. An electronic form for requesting exceptions to the U.S. citizenship requirement is published in *DHS 4300A Sensitive Systems Handbook*, Attachment J, "Requesting Exceptions to Citizenship Requirement."

Policy ID	DHS Policy Statements	Relevant Controls
1.5.4.a	Persons of dual citizenship, where one of the citizenships includes U.S. citizenship, shall be treated as U.S. citizens for the purposes of this Policy	---

Policy ID	DHS Policy Statements	Relevant Controls
	Directive.	
1.5.4.b	The System Owner shall submit each request for exception to the U.S. Citizenship policy to the Component Head. The Component Head shall obtain concurrence from the DHS Chief Security Officer (CSO) and CIO prior to the approval becoming effective.	PS-3
1.5.4.c	Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO.	PS-3

1.6 Electronic Signature

Pursuant to Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act,"[3] requires executive agencies to provide the option for electronic maintenance, submission, and disclosure of information when practicable as a substitute for paper, and to use and accept electronic signatures.

Electronic signatures are essential in the Department's business processes and IT environments; reducing reliance on paper transactions improves information sharing, strengthens information security, and streamlines business processes, while reducing both cost and environmental impact.

Electronic signature solutions must be approved by the Component CISO.

•

Policy ID	DHS Policy Statements	Relevant Controls
1.6.a	For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases, except where pen and ink signatures are required by public law, statute, Executive Order, or other agency requirement.	---
1.6.b	Wherever practicable, Components shall use and acceptance of electronic signatures.	---
1.6.c	Components shall accept electronic signatures whenever the signature's digital certificate is current, electronically verifiable, and issued by a medium or high assurance DHS Certification Authority (CA) or other medium or high CA under the Federal Bridge Certification Authority (FBCA) or Common Authority.	---
1.6.d	Components shall accept and be able to verify Personal Identity Verification (PIV) credentials issued by other Federal agencies as proof	---

[3] *Government Paperwork Elimination Act (GPEA), Pub L 105-277, 44 USC 3501 (note)provide for the use*

Policy ID	DHS Policy Statements	Relevant Controls
	of identity.	
1.6.e	As mandated by the Government Paperwork Elimination Act (GPEA) and OMB M-00-10, Components shall provide for the use and acceptance of electronic signatures when practicable.	---

1.7 Information Sharing

The DHS EOC exchanges information with Component SOCs, Network Operations Centers (NOC), the Homeland Secure Data Network (HSDN) SOC, the Intelligence Community, and with external organizations in order to facilitate the security and operation of the DHS network. This exchange enhances situational awareness and provides a common operating picture to network managers. The operating picture is developed from information obtained from "raw" fault, configuration management, accounting, performance, and security data. This data is monitored, collected, analyzed, processed, and reported by the NOCs and SOCs.

The DHS EOC is responsible for communicating other information such as incident reports, notifications, vulnerability alerts and operational statuses to Component SOCs, Component CISOs/ISSMs and other identified Component points of contact.

The DHS EOC portal implements role-based user profiles that allow Components to use the website's incident database capabilities. Users assigned to Component groups shall be able to perform actions such as:

- Entering incident information into the DHS EOC incident database
- Generating preformatted incident reports
- Initiating queries of the incident database
- Viewing FISMA incident reporting numbers
- Automating portions of the Information Security Vulnerability Management (ISVM) program

Automating portions of the vulnerability assessment program

1.8 Threats

Emphasis on e-Government has added the general public to the class of Government computer users and has transferred the repository for official records from paper to electronic media.

Information systems are often connected to different parts of an organization; interconnected with other organizations' systems; and with the Internet. Remote access for telecommuting and building management services (e.g., badge systems; heating, ventilating, and air-conditioning (HVAC); and entry) may require additional connections, all of which introduce additional risks.

Wireless systems such as cell phones, pagers, and other portable electronic devices (PED) allow personnel to stay in touch with their offices and wireless local area networks (WLAN) permit

connection from various locations throughout a building. While these technologies provide greater flexibility and convenience, they also introduce additional risks.

As technologies continue to converge, (cell phones with Internet access, walkie-talkie communications, and video; low cost Voice over Internet Protocol [VoIP]; copiers that allow network printing; printing over the Internet; , and facsimile [fax] functions) operating costs are reduced, making them tempting to implement, however each of these technology advancements contains inherent security risks and presents challenges to security professionals.

1.8.1 Internal Threats

Managers are generally aware of natural and physical threats, such as earthquakes, tornadoes, fires, floods, electric outages, and plumbing disasters, but may not have the same level of awareness regarding disasters or threats originating from within their organizations. The threat from DHS users should not be underestimated. Sensitive data can be lost, corrupted, or compromised through malicious or careless acts. A malicious user can intentionally cause harm to the Department's reputation and data. Uninformed or careless users can inflict similar damage.

Converging technologies combine the vulnerabilities of the individual technologies, so care must be taken to ensure that systems are designed with no single points of failure. (For example, if the building HVAC were connected to the data network it would become necessary to ensure that an outage or attack on the HVAC would not also cause a network outage.)

1.8.2 Criminal Threats

Malicious code remains a threat to DHS systems. Malware and those who employ it have become very sophisticated; malicious code can be tailored to the recipient. This code can be transferred to an unsuspecting user's machine by various means, including email, visiting infected websites, or across a network. These capabilities may be used to steal, alter, or destroy data; export malicious code to other systems; add backdoors that would permit access to data or network resources; or prevent the legitimate use of the individual computer or network service.

Instructions for exploiting hardware or software vulnerabilities are often available on hacker sites within hours of discovery. Skilled hackers routinely target e-commerce sites to obtain credit card numbers. Persons with hacking skills are often hired to perform espionage activities.

1.8.3 Foreign Threats

Foreign Governments routinely conduct espionage activities to obtain information that will be useful to their own industrial/government base and operations. They also have the resources to disrupt Internet communications and have launched successful cyber attacks.

Wireless communications are easily eavesdropped on using commercially available equipment, and it is relatively easy to detect and exploit wireless access points. Employees overseas should assume their wireless communications (BlackBerry, cell phone, etc) are being monitored.

Many software manufacturers outsource software code development, which raises concerns about whether malicious or criminal code has been inserted. Indeed, it is becoming increasingly difficult to determine the actual provenance of an organization's information systems because code and equipment are assembled from so many sources.

1.8.4 Lost or Stolen Equipment

Lost or stolen equipment also poses a threat. Data on portable computing devices (laptops, smart phones, etc) or storage media (Universal Serial Bus (USB) drives, compact disks (CD), etc) can reveal sensitive information, such as changes to legislation, investigations, or economic analyses. Thefts from offices, airports, automobiles, and hotel rooms occur regularly.

1.9 Changes to Policy

Procedures and guidance for implementing this policy are outlined in a companion publication, *DHS 4300A Sensitive Systems Handbook* and its attachments. The Handbook serves as a foundation for Components to use in developing and implementing their information security programs.

For interpretation or clarification of DHS information security policies found in this policy document and of the procedures and guidance found in the *DHS 4300A Sensitive Systems Handbook*, contact the DHS CISO at infosec@dhs.gov.

Changes to this policy and to the Handbook may be requested by submitting to the respective ISSM/CISO the form included in *DHS 4300A Sensitive Systems Handbook*, Attachment P, "Document Change Requests."

Policy ID	DHS Policy Statements	Relevant Controls
1.9.a	The DHS CISO shall be the authority for interpretation, clarification, and modification of the *DHS Sensitive Systems Policy Directive 4300A* and for the *DHS 4300A Sensitive Systems Handbook* (inclusive of all appendices and attachments).	PL-1
1.9.b	The DHS CISO shall update the *DHS Sensitive Systems Policy Directive 4300A* and the *DHS 4300A Sensitive Systems Handbook* at least annually.	PL-1

2.0 ROLES AND RESPONSIBILITIES

Security is inherently a Government responsibility; contractors, others working on behalf of the Department of Homeland Security (DHS), and other sources may assist in the performance of security functions, but a DHS employee must always be designated as the responsible agent for all security requirements and functions. This section outlines the roles and responsibilities for implementing these requirements.

2.1 Information Security Program Roles

Designated personnel play a major role in the planning and implementation of information security requirements. Roles directly responsible for information system security are described in the subsections that follow.

2.1.1 DHS Senior Agency Information Security Officer

Policy ID	DHS Policy Statements	Relevant Controls
2.1.1.a	The DHS Chief Information Security Officer (CISO) shall perform the duties and responsibilities of the DHS Senior Agency Information Security Officer (SAISO).	PL-1, PM-2

2.1.2 DHS Chief Information Security Officer

The DHS CISO shall implement and manage the DHS Information Security Program to ensure compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations.

The DHS CISO reports directly to the DHS Chief Information Officer (CIO) and is the principal advisor on information security matters.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.2.a	The DHS CISO shall implement and manage the DHS-wide Information Security Program.	PL-1, PM-2
2.1.2.b	The DHS CISO will serve as the CIO's primary liaison with the organization's Authorizing Officials (AO), information system owners and Information Systems Security Officers (ISSO).	---

The DHS CISO:

Implements and manages the Department-wide Information Security Program and ensures compliance with the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) directives, and other Federal requirements

- Issues Department-wide information security policy, guidance, and architecture requirements for all DHS systems and networks. These policies shall incorporate National Institute of Standards and Technology (NIST) guidance, as well as all applicable OMB memorandums and circulars

- Facilitates development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems
- Serves as the principal Departmental liaison with organizations outside DHS in matters relating to information security
- Reviews and approves the tools, techniques, and methodologies planned for use in certifying and authorizing DHS systems, and for reporting and managing systems-level FISMA data. This responsibility includes reviews and approval of Security Control Assessment plans, Contingency Plans, and security risk assessments.
- Consults with the DHS Chief Security Officer (CSO) on matters pertaining to physical security, personnel security, information security, investigations, and Sensitive Compartmented Information (SCI) systems, as they relate to information security and infrastructure
- Develops and implements procedures for detecting, reporting, and responding to information security incidents
- Ensures preparation and maintenance of plans and procedures to provide continuity of operations for information systems
- Ensures that Department personnel, contractors, and others working on behalf of DHS receive information security awareness training
- Chairs the CISO Council. The Council is composed of all Component CISOs, and is the Department's sole coordination body for any issues associated with information security policy, management, and operations. Component Information Systems Security Managers (ISSM) will be invited to CISO Council meetings as required
- Maintains a comprehensive inventory of all general support systems (GSS) and major applications (MA) in use within the Department
    - Security management for every GSS shall be under the direct oversight of either the DHS CISO (for enterprise systems) or a Component CISO/ISSM (for Component-specific GSSs)
    - MAs must be under the direct control of either a Component CISO or Component ISSM
- Maintains a repository for all Information Assurance (IA) security authorization process documentation and modifications
- Performs security reviews for all planned information systems acquisitions over $2.5 million and for additional selected cases
- Provides oversight of all security operations functions within the Department
- Maintains classified threat assessment capability in support of security operations
- Performs annual program assessments for each of the Components
- Performs periodic compliance reviews for selected systems and applications
- Publishes monthly Compliance Scorecards

- Delegates specific authorities and assigns responsibilities to Component CISOs and ISSMs, as appropriate for maintaining a high degree of compliance Reports annually to the Secretary on the effectiveness of the Department information security program, including progress of remedial actions. The CISO's annual report provides the primary basis for the Secretary's annual report to both OMB and to the United States Congress that is required by FISMA.
- Assists senior Department officials concerning their responsibilities under FISMA
- Heads an office with the mission and resources to assist in ensuring Department compliance with information security requirements
- Appoints a DHS employee to serve as the Headquarters CISO
- Appoints a DHS employee to serve as the Office of Intelligence and Analysis (I&A) CISO
- Provide operational direction to the DHS Security Operations Center (SOC)

2.1.3 Component Chief Information Security Officer

The Component CISO implements and manages all aspects of the Component Information Security Program to ensure compliance with DHS policy and guidance implementing FISMA, other laws, and Executive Orders. The Component CISO shall report directly to the Component CIO on matters relating to the security of Component information systems. In order to ensure continuity of operations and effective devolution, large Components should ensure the designation of a Deputy CISO with full authorities, to include the roles of Risk Executive and Security Control Assessor upon the absence of the CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.3.a	Component CISOs shall develop and maintain a Component-wide information security program in accordance with the DHS security program.	PL-1, PM-2
2.1.3.b	All Components shall be accountable to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO.	---

The following Components shall have a fulltime CISO:

- Customs and Border Protection (CBP)
- Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)
- United States Secret Service (USSS)
- United States Coast Guard (USCG)
- Federal Emergency Management Agency (FEMA)
- United States Citizenship and Immigration Services (USCIS)
- Federal Law Enforcement Training Center (FLETC)
- Headquarters, Department of Homeland Security

- Office of Intelligence and Analysis (I&A)
- National Protection and Programs Directorate (NPPD)

Component CISOs shall:

- Serve as principal advisor on information security matters
- Report directly to the Component CIO on matters relating to the security of Component information Systems
- Oversee the Component information security program
- Ensure that information security-related decisions and information, including updates to the 4300 series of information security publications, are distributed to the ISSOs and other appropriate persons within their Component
- Approve and/or validate all Component information system security reporting
- Consult with the Component Privacy Officer or Privacy Point of Contact (PPOC) for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Review and approve the security of hardware and software prior to implementation into the Component SOC
- Provide operational direction to the Component SOC
- Periodically test the security of implemented systems
- Implement and manage a Plan of Action and Milestones (POA&M) process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each information system managed at the Component level. Review and approve ISSO appointments
- Ensure that weekly incident reports are submitted to the DHS Enterprise Operations Center (EOC)
- Acknowledge receipt of Information System Vulnerability Management (ISVM) messages, report compliance with requirements or notify the granting of waivers
- Manage Component firewall rule sets
- Ensure that Interconnection Security Agreements (ISA) are maintained for all connections between systems that do not have the same security policy
- Ensure execution of the DHS Logging Strategy detailed in the *DHS 4300A Sensitive Systems Handbook*
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1, *DHS 4300A Sensitive Systems Handbook*)

- Ensure reporting of vulnerability scanning activities to the DHS EOC, in accordance with *DHS 4300A Sensitive Systems Handbook* Attachment O, "Vulnerability Management Program."
- Develop and maintain a Component-wide information security program in accordance with Department policies and guidance
- Implement Department information security policies, procedures, and control techniques to ensure that all applicable requirements are met
- Update Security Training section within DHS FISMA Manager resource at least once per quarter
- Ensure training and oversight of personnel with significant responsibilities for information security
- Oversee the Component's Security Authorization process for GSSs and MAs
- Maintain an independent Component-wide assessment program to ensure that there is a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the assessment process for each authorized application
- Ensure that enterprise security tools are utilized
- Oversee all Component security operations functions, including the Component SOCs
- Ensure that external providers who operate information systems on behalf of the Component meet the same security requirements as required for information and information systems.
- Ensure an acceptable level of trust in the external service; or using compensating controls to secure information or the process flow, accepting a greater degree of risk, or reducing the functionality to the extent necessary to make the risk acceptable

Component CISO qualifications include:

- Training, experience, and professional skills required to discharge the responsibilities and functions of the position
- Ability to maintain a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance
- Ability to perform information security duties as primary duty
- Ability to participate in the DHS CISO Council
- Ability to head an office with the mission and resources to ensure the Component's compliance with this Policy Directive
- Ability to coordinate, develop, implement, and maintain an organization-wide information security program
- Ability to serve as the Component Risk Executive

2.1.4 Component Information Systems Security Manager

Components that are not required to have a fulltime CISO shall have a fulltime ISSM. The ISSM is designated in writing by the Component CIO, with the concurrence of the DHS CISO.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.4.a	Component ISSMs shall serve as the principal interface between the HQ CISO, Component ISSOs and other security practitioners.	---
2.1.4.b	The Component ISSM shall work directly with the HQ CISO.	---

The ISSM plays a critical role in ensuring that the DHS Information Security Program is implemented and maintained throughout the Component.

Component ISSMs:

- Oversee the Component information security program
- Ensure that the Component CIO and DHS CISO are kept informed of all matters pertaining to the security of information systems
- Ensure that all communications and publications pertaining to information security, including updates to the 4300 Policies and Handbooks, are distributed to the ISSOs and other appropriate persons within their Component
- Validate all Component information system security reporting
- Consult with the Component Privacy Officer or PPOC for reporting and handling of privacy incidents
- Manage information security resources including oversight and review of security requirements in funding documents
- Test the security of the Component's information systems periodically
- Implement and manage a POA&M process for remediation by creating a POA&M for each known vulnerability
- Ensure that ISSOs are appointed for each Component-managed information system
- Ensure that weekly incident reports are forwarded to the HQ CISO
- Acknowledge receipt of ISVM messages, report compliance with requirements, or notify applicants of the granting of waivers
- Ensure adherence to the DHS Secure Baseline Configuration Guides (Enclosure 1, *DHS 4300A Sensitive Systems Handbook*)
- Develop and publish procedures for implementation of DHS information security policy within the Component
- Implement Department information security policies, procedures, and control techniques to address all applicable requirements
- Ensure training and oversight for personnel with significant responsibilities for information security
    - Oversee the Security Authorization process for the Component's MAs

- Maintain an independent Component-wide security control assessment program to ensure a consistent approach to controls effectiveness testing
- Ensure that an appropriate SOC performs an independent network assessment as part of the security control assessment process for each authorized application
- Ensure that enterprise security tools are used

2.1.5 Risk Executive

A Risk Executive ensures that risks are managed consistently across the organization. In keeping with its organizational structure, DHS has two levels of Risk Executive: Departmental and Component. The risk executive provides a holistic view of risk beyond that associated with the operation and use of individual information systems. Risk Executive observations and analyses are documented and become part of the security authorization decision.

All DHS Risk Executives:

- Ensure that management of security risks related to information systems is consistent throughout the organization; reflects organizational risk tolerance; and is performed as part of an organization-wide process that considers other organizational risks affecting mission and business success
- Ensure that information security considerations for individual information systems, including the specific authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization
- Provide visibility into the decisions of AOs and a holistic view of risk to the organization beyond the risk associated with the operation and use of individual information systems
- Facilitate the sharing of security-related and risk-related information among AOs and other senior leaders in the organization in order to help those officials consider all types of risks that could affect mission and business success and the overall interests of the organization at large

The DHS Risk Executive develops information security policy, establishes the standards for system security risk, oversees risk management and monitoring, and approves all waivers and exceptions to DHS policy.

Component Risk Executives may establish system security risk standards more stringent than DHS standards. Risk Executives implement the system security risk management and monitoring program and submit requests for higher-risk deviations from the enterprise standard.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.a	The DHS CIO shall be the DHS Risk Executive. (The DHS CISO has been designated by the DHS CIO as the Risk Executive.)	PL-1, PM-9
2.1.5.b	Each Component CISO shall be the Risk Executive for his or her Component.	PL-1, PM-9

Policy ID	DHS Policy Statements	Relevant Controls
2.1.5.c	The Risk Executive shall perform duties in accordance with NIST Special Publication (SP) 800-37.	---

2.1.6 Authorizing Official

The AO formally assumes responsibility for operating an information system at an acceptable level of risk. He or she shall be a senior management official and a Federal employee or member of the U.S. military. The AO shall assign the Security Control Assessor for the system.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.6.a	The DHS CIO shall act as the AO for enterprise information systems or shall designate an AO in writing.	CA-6
2.1.6.b	The Component CIO shall act as the AO for Component information systems or shall designate an AO in writing.	CA-6
2.1.6.c	Every system shall have a designated AO. (An AO may be responsible for more than one system.)	CA-6
2.1.6.d	The AO shall be responsible for review and approval of any individual requiring administrator privileges. The AO may delegate the performance of this duty to the appropriate system owner or Program Manager.	AC-2
2.1.6.e	The AO shall be responsible for acceptance of remaining risk to organizational operations and assets, individuals, other organizations, and the Nation.	CA-6
2.1.6.f	The AO shall periodically review security status for all systems under his or her purview to determine if risk remains acceptable	CA-6
2.1.6.g	The AO shall perform additional duties in accordance with NIST SP 800-37	CA-6

2.1.7 Security Control Assessor

The Security Control Assessor is a senior management official whose responsibilities include certifying the results of the security control assessment. A Security Control Assessor, who must be a Federal employee, is assigned in writing to each information system by an appropriate Component official, typically the Component Head or Component CIO. The Security Control Assessor and the team conducting a certification must be impartial. They must be free from any perceived or actual conflicts of interest with respect to the developmental, operational, and or management chains of command associated with the information system; or with respect to the determination of security control effectiveness.

For systems with low impact, a Security Control Assessor and/or certifying team does not need to be independent so long as assessment results are carefully reviewed and analyzed by an independent team of experts to validate their completeness, consistency, and truthfulness.

The AO decides the required level of assessor independence based on:

- The criticality and sensitivity of the information system
- The ultimate risk to organizational operations, organizational assets, and individuals
- The level of assessor independence required for confidence that the assessment results are sound and valid for making credible risk-based decisions.

Policy ID	DHS Policy Statements	Relevant Controls
2.1.7.a	The Component CISO shall serve as Security Control Assessor when no other person has been officially designated.	CA-2
2.1.7.b	A Security Control Assessor may be responsible for more than one system.	CA-2
2.1.7.c	The Security Control Assessor may take the lead for any or all remedial actions.	CA-7
2.1.7d	The Security Control Assessor provides an assessment of the severity of weaknesses or deficiencies in the information systems, and prepares the final security control assessment report containing the results and findings from the assessment but not making a risk determination.	CA-7

2.1.8 Information Systems Security Officer

An ISSO performs security actions for an information system. Only one ISSO is assigned to a system, but multiple Alternate ISSOs may be designated to assist the ISSO.

While the ISSO performs security functions, responsibility for information system security always rests with the System Owner.

See *DHS 4300A Sensitive Systems Handbook*, Attachment C, "Information Systems Security Officer (ISSO) Designation Letter."

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.a	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
2.1.8.b	An ISSO shall ensure the implementation and maintenance of security controls in accordance with the Security Plan (SP) and DHS policies.	PL-1
2.1.8.c	An ISSO may be a DHS employee or a contractor.	PL-1

Policy ID	DHS Policy Statements	Relevant Controls
2.1.8.d	An ISSO may be assigned to more than one system.	PL-1
2.1.8.e	ISSO duties shall not be assigned as collateral duties unless approved by the Component CISO.	PL-1
2.1.8.f	The ISSO shall have been granted a clearance and access greater than or equal to the highest level of information contained on the system. The minimum clearance for an ISSO shall be Secret.	---
2.1.8.g	The ISSO shall ensure that timely responses are provided to Infrastructure Change Control Board (ICCB) change request packages.	---

2.2 Other Roles

Roles related to, but not directly responsible for, information system security are described in the subsections that follow.

2.2.1 Secretary of Homeland Security

The Secretary of Homeland Security is responsible for fulfilling the Department's mission, which includes ensuring that DHS information systems and their data are protected in accordance with Congressional and Presidential directives. The Secretary's role with respect to information system security is to allocate adequate resources.

To that end, the Secretary:

- Ensures that DHS implements its Information Security Program throughout the life cycle of each DHS system
- Submits the following to the Director, OMB:
    - the DHS CIO's assessment of the adequacy and effectiveness of the Department's information security procedures, practices, and FISMA compliance,
    - the results of an annual independent information security program evaluation performed by the DHS Office of Inspector General (OIG)
    - the Senior Agency Official for Privacy's (SAOP) annual assessment of the Department's privacy policies, procedures, and practices to the Director, OMB
- Provides information security protection commensurate with the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the Department, and on information systems used or operated by the Department, or by a contractor or other organization on behalf of the Department
- Ensures that an information security program is developed, documented, and implemented to provide security for all systems, networks, and data that support the Department's operations

- Ensures that information security processes are integrated with strategic and operational planning processes to secure the Department's mission
- Ensures that the Department's senior officials have the necessary authority to secure the operations and assets under their control
- Delegates authority to the CIO to ensure compliance with applicable information security requirements

2.2.2 Under Secretaries and Heads of DHS Components

The Under Secretaries and Heads of DHS Components are responsible for oversight of their Components' information security program, including the appointment of CIOs. Undersecretaries and Heads of Components allocate adequate resources to information systems for information system security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.2.a	The Under Secretaries of Homeland Security and Heads of Components shall ensure that information systems and their data are sufficiently protected.	PL-1

Under Secretaries and the Heads of DHS Components:

- Appoint CIOs
- Ensure that an Information Security Program is established and managed in accordance with DHS policy and implementation directives
- Ensure that the security of information systems is an integral part of the life cycle management process for all information systems developed and maintained within their Components
- Ensure that adequate funding for information security is provided for Component information systems and that adequate funding requirements are included for all information systems budgets
- Ensure that information system data are entered into the appropriate DHS Security Management Tools to support DHS information security oversight and FISMA reporting requirements
- Ensure that the requirements for an information security performance metrics program are implemented and the resulting data maintained and reported

2.2.3 DHS Chief Information Officer

The DHS CIO is the senior agency executive responsible for all DHS information systems and their security as well as for ensuring FISMA compliance.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.3.a	The DHS CIO shall develop and maintain the DHS Information Security Program.	PL-1
2.2.3.b	The DHS CIO designates the DHS CISO.	PL-1

The DHS CIO:

- Heads an office with the mission and resources to assist in ensuring Component compliance with the DHS Information Security Program
- Oversees the development and maintenance of a Department-wide information security program
- Appoints in writing a DHS employee to serve as the DHS CISO
- As appropriate, serves as or appoints in writing the AO for DHS enterprise information systems.
- Participates in developing DHS performance plans, including descriptions of the time periods and budget, staffing, and training resources required to implement the Department-wide security program
- Ensures that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensures that DHS security programs integrate fully into the DHS enterprise architecture and capital planning and investment control processes
- Ensures that System Owners understand and appropriately address risks, including interconnectivity with other programs and systems outside their control
- Reviews and evaluates the DHS Information Security Program annually
- Ensures that an information security performance metrics program is developed, implemented, and funded
- Reports to the DHS Under Secretary for Management on matters relating to the security of DHS systems
- Ensures compliance with applicable information security requirements
- Coordinates and advocates resources for enterprise security solutions
- Leads the DHS Contingency Planning program

2.2.4 Component Chief Information Officer

The Component CIO is responsible for Component information systems and their security as well as for ensuring FISMA compliance within the Component.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.4.a	The Component CIO shall develop and maintain the Component Information Security Program.	PL-1, PM-1

Component CIOs:

- Establish and oversee their Component information security programs
- Ensure that an AO has been appointed for every Component information system; serves as the AO for any information system for which no AO has been appointed or where a vacancy exists
- Ensure that information security concerns are addressed by Component Configuration Control Boards, Enterprise Architecture Board (EAB), and Acquisition Review Board (ARB)/Investment Review Board (IRB)
- Ensure that an accurate information systems inventory is established and maintained
- Ensure that all information systems acquisition documents, including existing contracts, include appropriate information security requirements and comply with DHS information security policies
- Ensure that System Owners understand and appropriately address risks, including risks arising from interconnectivity with other programs and systems outside their control
- Ensure that an information security performance metrics program is developed, implemented, and funded
- Advise the DHS CIO of any issues regarding infrastructure protection, vulnerabilities or the possibility of public concern
- Ensure that incidents are reported to the DHS EOC within reporting time requirements as defined in Attachment F, "" of the *DHS Sensitive Systems Handbook*
- Work with the DHS CIO and Public Affairs Office in preparation for public release of security incident information. The DHS CIO, or designated representative, has sole responsibility for public release of security incident information.
- Ensure compliance with DHS information systems security policy
- Coordinate and advocate resources for information security enterprise solutions

CIOs of the following Components shall appoint a CISO that reports directly to the Component CIO and shall ensure that the CISO has resources to assist with Component compliance with policy. CISOs shall be DHS employees.

- CBP
- FEMA
- FLETC
- ICE

- TSA
- USCIS
- USCG
- USSS

CIOs of all other Components shall:

- Ensure that Component ISSMs have been appointed
- Provide the resources and qualified personnel to ensure Component compliance with DHS security policy

2.2.5 DHS Chief Security Officer

The DHS Chief Security Officer (CSO) implements and manages the DHS Security Program for DHS facilities and personnel.

The CSO is a senior agency official who reports directly to the Deputy Secretary on all matters pertaining to facility and personnel security within the DHS.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.5.a	DHS information systems that control physical access shall be approved by the DHS CSO to operate in accordance with this policy document, whether they connect to other DHS information systems or not.	CA-1
2.2.5.b	The DHS CSO shall be the AO for all systems automating or supporting physical access controls or shall appoint an AO for each of those systems.	CA-6

2.2.6 DHS Chief Privacy Officer

The DHS Chief Privacy Officer is the head of the DHS Privacy Office and is responsible for creation of privacy policies and their implementation in all Components of the Department. The responsibilities of the DHS Chief Privacy Officer include oversight of all privacy activities within the Department, and ensuring compliance with privacy policies.

The DHS Chief Privacy Officer assists Component Privacy Officers and Privacy PPOC with policy compliance at the Component level.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.6.a	The Chief Privacy Officer shall review program and system Privacy Threshold Analyses (PTA), Privacy Impact Assessments (PIA), and System of Records Notices (SORN), providing approval as appropriate.	PL-1, PL-5

The Chief Privacy Officer, as the senior privacy official:

- Oversees privacy incident management
- Responds to suspected or confirmed privacy incidents
- Coordinates with the DHS CIO, DHS CISO, the DHS EOC, and senior management regarding privacy incidents
- Convenes and chairs incident response teams, such as the Privacy Incident Response Team (PIRT) and the Core Management Group (CMG)
- Approves program and system PTAs, PIAs, and SORNs
- Designates Privacy Sensitive Systems based on validated PTAs. Privacy Sensitive Systems are those that maintain Personally Identifiable Information (PII)
- Provides Department-wide annual and refresher privacy training

2.2.7 DHS Chief Financial Officer

The DHS Chief Financial Officer (CFO) implements and manages the DHS Financial Program, including oversight of DHS financial systems. The DHS CFO designates financial systems and oversees security control definitions for financial systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.7.a	The DHS CFO shall be the AO for all financial systems managed at the DHS level.	CA-6
2.2.7.b	The DHS CIO has directed that the Component CFO shall be the AO for all financial mission applications managed at the Component level.	CA-6
2.2.7.c	The DHS CFO shall designate the financial systems that fall under the DHS CFO-mandated policy statements.	CA-6
2.2.7.d	The DHS CFO shall publish a comprehensive list of designated financial systems during the fourth quarter of every fiscal year. (This list shall be referred to as the CFO Designated Systems List.)	CA-6

All systems on the CFO Designated Systems List are required to comply with the policies defined in Sections 3.5.1 and 3.15.

2.2.8 Program Managers

Program Managers ensure compliance with applicable Federal laws and DHS policy directives governing the security, operation, maintenance, and privacy protection of information systems, information, projects, and programs under their control.

Program Managers are responsible for program-level POA&Ms that may impact one or more systems.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.8.a	Program Managers shall ensure that program POA&Ms are prepared and maintained.	CA-5, PM-4
2.2.8.b	Program Managers shall prioritize security weaknesses for mitigation.	CA-5
2.2.8.c	Program Managers shall provide copies of program POA&Ms to affected System Owners.	CA-5, PM-4
2.2.8.d	Program Managers shall ensure that POA&Ms address the following: ▪ known vulnerabilities in the information system ▪ the security categorization of the information system ▪ the specific weaknesses or deficiencies in the information system security controls ▪ the importance of the identified security control weakness or deficiencies ▪ the Component's proposed risk mitigation approach while addressing the identified weaknesses or deficiencies in the security controls the rationale for accepting certain weaknesses or deficiencies in the security controls.	CA-5

2.2.9 System Owners

System Owners use Information Technology (IT) to help achieve the mission needs within their program area of responsibility. They are responsible for the successful operation of the information systems and programs within their program area and are ultimately accountable for their security. All systems require a System Owner designated in writing for proper administration of security.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.a	System Owners shall ensure that each of their systems is deployed and operated in accordance with this policy document.	PL-1
2.2.9.b	System Owners shall ensure that an ISSO is designated in writing for each information system under their purview.	PL-1
2.2.9.c	There shall be only one System Owner designated for each DHS system.	PL-1
2.2.9.d	The System Owner shall ensure information security compliance, development and maintenance of security plans, user security training, notifying officials of the need for security authorization and need to resource.	CA-2

Policy ID	DHS Policy Statements	Relevant Controls
2.2.9.e	System Owners shall ensure development of a POA&M to address weaknesses and deficiencies in the information system and its operating environment.	CA-2

2.2.10 Common Control Provider

The Common Control Provider is an organizational official responsible for planning, development, implementation, assessment, authorization, and maintenance of common controls.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.10.a	The Common Control Provider shall document all common controls and submit them to the AO and DHS CISO.	PM-1
2.2.10.b	The Common Control Provider ensures that required assessments of common controls are carried out by qualified assessors with the appropriate level of independence.	PM-1
2.2.10.c	The Common Control Provider documents assessment findings in a security assessment report (SAR).	PM-1
2.2.10.d	The Common Control Provider ensures that POA&Ms are developed for all controls having weaknesses or deficiencies.	PM-4
2.2.10.e	The Common Control Provider shall make available security plans, SARs, and POA&Ms for common controls to information system owners inheriting those controls after the information is reviewed and approved by a senior official.	PM-1, PM-4

2.2.11 DHS Employees, Contractors, and Others Working on Behalf of DHS

DHS employees, contractors, and others working on behalf of the DHS or its agencies shall follow the appropriate set(s) of rules of behavior.

Policy ID	DHS Policy Statements	Relevant Controls
2.2.11.a	DHS users shall follow prescribed rules of behavior.	PL-4

3.0 MANAGEMENT POLICIES

3.1 Basic Requirements

Basic security management principles must be followed in order to ensure the security of Department of Homeland Security (DHS) information resources. These principles are applicable throughout the Department and form the cornerstone of the DHS Information Security Program.

Component Chief Information Security Officers (CISO) and Information Systems Security Managers (ISSM) shall submit all security reports concerning DHS systems to the Component senior official or designated representative. Component CISOs/ISSMs shall interpret and manage DHS security policies and procedures to meet Federal, Departmental, and Component requirements. Component CISOs/ISSMs shall also answer data queries from the DHS CISO and develop and manage information security guidance and procedures unique to Component requirements.

Information Systems Security Officers (ISSO) are the primary points of contact for the information systems assigned to them. They develop and maintain Security Plans (SP) and are responsible for overall system security.

Policy ID	DHS Policy Statements	Relevant Controls
3.1.a	Every DHS computing resource (desktop, laptop, server, portable electronic device, etc.) shall be individually accounted for as part of a FISMA[4]-Inventoried information system.	CM-8
3.1.b	The Component Chief Information Officer (CIO), in cooperation with each of the Component's senior officials, shall be responsible for ensuring that every DHS computing resource is identified as an information system or as a part of an information system, either as an MA or as a general support system (GSS).	CM-8
3.1.c	The System Owner or designee shall develop and maintain a Security Plan (SP) for each information system. Component Authorizing Officials (AO) shall review and approve SPs.	PL-2
3.1.d	An ISSO shall be designated for every information system and serve as the point of contact (POC) for all security matters related to that system.	PL-1
3.1.e	Component information security programs shall be structured to support DHS and applicable FISMA, Office of Management and Budget (OMB), and other Federal requirements.	PL-1
3.1.f	Information security reports regarding DHS systems shall be submitted to the Senior Component official or designated representative.	---
3.1.g	Component CISOs/ISSMs shall ensure that their information systems comply with the DHS Enterprise Architecture (EA) Technical Reference Model	PL-1,

[4] *FISMA: Federal Information Security Management Act, 44 U.S.C. 3541*

Policy ID	DHS Policy Statements	Relevant Controls
	(TRM) and Security Architecture (SA) or maintain a waiver, approved by the DHS CIO/ CISO.	PM-1
3.1.h	The DHS CISO shall issue Department-wide information security policy, guidance, and information security architecture requirements for all DHS systems.	CM-2, CM-6
3.1.i	Component CISOs shall implement DHS information security policies, procedures, and control techniques to meet all applicable requirements.	PL-1, PM-1
3.1.j	Component CISOs shall develop and manage information security guidance and procedures unique to Component requirements.	PL-1, PM-1

3.2 Capital Planning and Investment Control

Information security is a business driver and any risks found through security testing are ultimately business risks. Information security personnel should be involved, to the maximum extent possible, in all aspects of the acquisition process, including drafting contracts, and procurement documents. DHS Management Directive (MD) 102-01, *Acquisition Management Directive* and DHS MD 4200.1, *IT Capital Planning and Investment Control (CPIC) and Portfolio Management* provide additional information on these requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.2.a	System Owners shall include information security requirements in their CPIC business cases for the current budget year and for the Future Years Homeland Security Program (FYHSP) for each DHS system.	PM-3, PM-11, SA-1
3.2.b	System Owners or AOs shall ensure that information security requirements and Plans of Action and Milestones (POA&M) are adequately funded, resourced and documented in accordance with current OMB budgetary guidance.	PM-3, PM-4, SA-2
3.2.c	Component IRBs/ARBs shall not approve any capital investment in which the information security requirements are not adequately defined and funded.	PM-3, SA-2
3.2.d	The DHS CISO shall perform security reviews for planned information system acquisitions over $2.5 million, and in selected additional cases.	SA-1
3.2.e	Components shall ensure that information security requirements as described in this Policy Directive are met in the acquisition of all DHS systems and services used to input, process, store, display, or transmit sensitive information.	SA-4

Policy ID	DHS Policy Statements	Relevant Controls
3.2.f	Procurement authorities throughout the Department shall enforce the provisions of the Homeland Security Acquisition Regulation (HSAR).	SA-1, SA-4
3.2.g	Procurements for services and products involving facility or system access control shall be in accordance with DHS guidance regarding HSPD-12 implementation.	—

3.3 Contractors and Outsourced Operations

Policy ID	DHS Policy Statements	Relevant Controls
3.3.a	All Statements of Work (SOW) and contract vehicles shall identify and document the specific security requirements for information system services and operations required of the contractor.	SA-4
3.3.b	Contractor information system services and operations shall adhere to all applicable DHS information security policies.	SA-9
3.3.c	Requirements shall address how sensitive information is to be handled and protected at contractor sites, including any information stored, processed, or transmitted using contractor information systems. Requirements shall also include requirements for personnel background investigations and clearances, and facility security.	SA-9
3.3.d	SOWs and contracts shall include a provision stating that, when the contract ends, the contractor shall return all information and information resources provided during the life of the contract and certify that all DHS information has been purged from any contractor-owned system(s) that have been used to process DHS information.	SA-4
3.3.e	Components shall conduct reviews to ensure that information security requirements are included in contract language and that the requirements are met throughout the life of the contract.	SA-1
3.3.f	Security deficiencies in any outsourced operation shall require creation of a program-level POA&M.	SA-9, PM-4

3.4 Performance Measures and Metrics

Policy ID	DHS Policy Statements	Relevant Controls
3.4.a	The DHS CISO shall define performance measures to evaluate the effectiveness of the DHS information security program.	—

Policy ID	DHS Policy Statements	Relevant Controls
3.4.b	Components shall provide OMB FISMA data at least monthly to the DHS Compliance Officer.	---
3.4.c	The DHS CISO shall report annually to the Secretary on the effectiveness of the DHS information security program, including the progress of remedial actions.	---
3.4.d	Components shall use the automated tool specified by the DHS CISO for Performance Plan reporting.	---
3.4.e	The DHS CISO shall collect OMB FISMA data from Components at least quarterly and provide FISMA reports to OMB.	---

3.5 Continuity Planning for Critical DHS Assets

The Continuity Planning for Critical DHS Assets Program is vital to the success of the DHS Information Security Program. The Business Impact Assessment (BIA) is essential in the identification of critical DHS assets. Once critical systems are identified, continuity planning shall address the following two different but complementary elements:

- Continuity of Operations Planning (COOP)
- Contingency Planning (CP)

3.5.1 Continuity of Operations Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.1.a	When available, a DHS-wide process for continuity of operations (CO) planning shall be used in order to ensure continuity of operations under all circumstances.	CP-2
3.5.1.b	Components shall develop, test, implement, and maintain comprehensive Continuity of Operations Plans (COOP) to ensure the recovery and continuity of essential DHS functionalities.	CP-2, CP-4
3.5.1.c	All CISOs/ISSMs shall ensure that all COOPs under their purview are tested and exercised annually.	CP-4
3.5.1.d	All Chief Financial Officer (CFO)- Designated Systems requiring high availability shall be identified in COOP plans and exercises.	CP-1
3.5.1.e	All personnel involved in COOP efforts shall be identified and trained in the procedures and logistics of COOP development and implementation.	AT-3, CP-3
3.5.1.f	To ensure that accounts can be created in the absence of the usual account approval authority, systems that are part of the Critical DHS Assets Program	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
	shall have provisions to allow a Component CISO/ISSM or Component CIO to approve new user accounts as part of a COOP scenario.	
3.5.1.g	Each Component shall compile and maintain a list of mission-critical information systems in support of COOP.	CM-8, CP-1
3.5.1.h	The DHS and Component CISOs/ISSMs shall ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems.	CP-1
3.5.1.i	DHS information systems that are part of the DHS Continuity Planning for Critical DHS Assets Program shall be provided requirements for system-level contingency planning by a Component Contingency Planning Program Office or by a DHS Contingency Planning Program Office.	---

3.5.2 Contingency Planning

Policy ID	DHS Policy Statements	Relevant Controls
3.5.2.a	The DHS CIO shall provide guidance, direction, and authority for a standard DHS-wide process for contingency planning for information systems.	CP-1
3.5.2.b	System Owners shall develop and document information system Contingency Plans (CPs) for their programs, manage plan changes, and distribute copies of the plan to key contingency personnel. Component CIOs shall review and approve Component-level information system CPs.	CP-1, CP-2
3.5.2.c	Components shall ensure implementation of backup policy and procedures for every Component information system.	CP-9
3.5.2.d	The DHS CIO shall ensure that each DHS system has contingency capabilities commensurate with the ***availability*** security objective. The minimum contingency capabilities for each impact level are as follows: **High impact** – System functions and information have a high priority for recovery after a short period of loss. **Moderate impact** – System functions and information have a moderate priority for recovery after a moderate period of loss. **Low impact** – System functions and information have a low priority for recovery after prolonged loss.	CP-1
3.5.2.e	CPs shall be developed and maintained by all DHS Components in accordance with the requirements for the FIPS 199 potential impact level for the **availability** security objective. These plans shall be based on three essential phases: Activation/Notification, Recovery, and Reconstitution. Components shall review the CP for the information system at least annually and revise the plan to address system/organizational changes or problems encountered during	CP-1, CP-2

Policy ID	DHS Policy Statements	Relevant Controls
	plan implementation, execution, or testing.	
3.5.2.f	The DHS CIO shall ensure that CP testing is performed in accordance with the **availability** security objective. The minimum contingency testing for each impact level follows: **High impact** – System recovery roles, responsibilities, procedures, and logistics in the CP shall be used within a year prior to authorization to recover from a simulated contingency event at the alternate processing site. The system recovery procedures in the CP shall be used at least annually to simulate system recovery in a test facility. **Moderate impact** – The CP shall be tested at least annually by reviewing and coordinating with organizational elements responsible for plans within the CP. This is achieved by performing a walk-through/tabletop exercise. **Low impact** – CP contact information shall be verified at least annually.	CP-4, CP-7
3.5.2.g	The DHS CIO shall ensure that contingency training is performed in accordance with the **availability** security objective. The minimum contingency planning for each impact level follows: **High impact** – All personnel involved in contingency planning efforts shall be identified and trained in their contingency planning and implementation roles, responsibilities, procedures, and logistics. This training shall incorporate simulated events. Refresher training shall be provided at least annually. **Moderate impact** – All system personnel involved in contingency planning efforts shall be trained. Refresher training shall be provided at least annually. **Low impact** – There is no training requirement.	CP-3
3.5.2.h	Components shall coordinate CP testing and/or exercises as appropriate, using COOP-related plans for systems with moderate and high availability FIPS-199 categorization.	CP-4

3.6 Systems Engineering Life Cycle

The DHS Systems Engineering Life Cycle (SELC) is detailed in Acquisition Management Directive 102-01, Appendix B.

Policy ID	DHS Policy Statements	Relevant Controls
3.6.a	Components shall ensure that system security is integrated into all phases of SELC.	SA-3
3.6.b	Components shall ensure that security requirements for sensitive information systems are incorporated into life-cycle documentation.	SA-3
3.6.c	The Program Manager shall review, approve, and sign all custom-developed code prior to deployment into production environments. The Program Manager may delegate this authority in writing to another DHS employee.	RA-5

Policy ID	DHS Policy Statements	Relevant Controls
	The authority shall not be delegated to contractor personnel.	

3.7 Configuration Management

Configuration Management (CM) includes management of all hardware and software elements of information systems and networks. CM within DHS consists of a multi-layered structure – policy, procedures, processes, and compliance monitoring. Each Component shall use an appropriate level of configuration management.

CM applies to all systems, subsystems, and components of the DHS infrastructure, and ensures implementation and continuing life-cycle maintenance. CM begins with baselining of requirements documentation and ends with decommissioning of items no longer used for production or support.

The CM discipline applies to hardware, including power systems, software, firmware, documentation, test and support equipment, and spares. A Change Management Process ensures that documentation associated with an approved change to a DHS system is updated to reflect the appropriate baseline, including an analysis of any potential security implications. The initial configuration must be documented in detail and all subsequent changes must be controlled through a complete and robust CM process.

Configuration management has security implications in three areas:

- Ensuring that the configuration of subordinate information system elements is consistent with the Security Authorization Process requirements of the parent system
- Ensuring that any subsequent changes (including an analysis of any potential security implications) are approved
- Ensuring that all recommended and approved security patches are properly installed

Enclosure 1 of *DHS Sensitive Systems Handbook* includes the DHS Secure Baseline Configuration Guides.

Policy ID	DHS Policy Statements	Relevant Controls
3.7.a	Components shall develop and maintain a configuration management plan (CMP) for each information system as part of its SP. All DHS systems shall be under the oversight of the officer responsible for Configuration Management.	CM-1, CM-9
3.7.b	Components shall establish, implement, and enforce configuration management controls on all information systems and networks and address significant deficiencies as part of a POA&M.	CA-5, CM-3, PM-4
3.7.c	Information security patches shall be installed in accordance with configuration management plans and within the timeframe or direction stated in the Information Security Vulnerability Management (ISVM) message	SI-2

Policy ID	DHS Policy Statements	Relevant Controls
	published by the DHS Enterprise Operations Center (EOC).	
3.7.d	System Owners shall document initial system configuration in detail and shall control all subsequent changes in accordance with the configuration management process.	CM-2, CM-3, CM-9
3.7.e	Workstations shall be configured in accordance with DHS guidance on the U.S Government Configuration Baseline (USGCB) (formerly known as the Federal Desktop Core Configuration [FDCC]). Configuration shall include installation of the DHS Common Policy Object identifier (OID), Common Policy Framework Root CA certificate, and the DHS Principal CA certificate.	CM-2, CM-6, CM-9
3.7.f	Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool.	---
3.7.g	The System Owner shall request an exception for information systems that use operating systems or applications that are not hardened or do not follow configuration guidance identified in Enclosure 1 of *DHS Sensitive Systems Handbook* DHS Secure Baseline Configuration Guides. Requests shall include a proposed alternative secure configuration.	CM-2, CM-6
3.7.h	Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes.	CM-4

3.8 Risk Management

Risk management is a process that allows System Owners to balance the operational and economic costs of protective measures to achieve gains in mission capability by protecting the information systems and data that support their organization's missions.

Policy ID	DHS Policy Statements	Relevant Controls
3.8.a	Components shall establish a risk management program in accordance with NIST Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems* and with other applicable Federal guidelines.	RA-1
3.8.b	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever major modifications that have the potential to significantly impact risk are made to sensitive information systems, or to their physical environments, interfaces, or user community. The risk assessment shall consider the effects of the modifications on the operational risk profile of the information system. SPs shall be updated and re-certification conducted if warranted by the results of the risk assessment.	RA-3
3.8.c	Each Component CISO/ISSM shall establish an independent Component-wide	RA-1

Policy ID	DHS Policy Statements	Relevant Controls
	Security Authorization program to ensure a consistent approach to testing the effectiveness of controls.	
3.8.d	Risk Executives shall review recommendations for risk determinations and risk acceptability and may recommend changes to the AO and appropriate CIO.	RA-3
3.8.e	Component Security Operations Centers (SOC) shall deploy a Component-wide network scanning program.	RA-5
3.8.f	Special rules apply to CFO-Designated Systems. See Section 3.15 for additional information.	---

3.9 Security Authorization and Security Control Assessments

DHS periodically assesses the selection of security controls to determine their continued effectiveness in providing an appropriate level of protection.

It is recommended that Components pursue type *Security Authorization Process* for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments.

Type *Security Authorization Process* shall consist of a master *Security Authorization Process* package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.

The DHS *Security Authorization Process Guide* describes detailed processes governing *Security Authorization Process* and system risk assessment.

Detailed information for creating and managing POA&Ms is published in DHS 4300A *Sensitive Systems Handbook, Attachment H – Plan of Action and Milestones (POA&M) Process Guide.*

Policy ID	DHS Policy Statements	Relevant Controls
3.9.a	Components shall assign an impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) for each DHS information system. Components shall apply NIST SP 800-53 controls as tailored specifically to the security objective at the determined impact level in the Attachment M to *DHS 4300A, Sensitive Systems Handbook*, "Tailoring the NIST 800-53 Security Controls."	PM-10, RA-2
3.9.b	Components shall implement NIST SP 800-53 security controls, using the FIPS Pub 200, *Minimum Security Requirements for Federal Information and Information Systems* methodology, based on the FIPS 199 impact level established for each separate security objective (confidentiality, integrity, availability).	---

Policy ID	DHS Policy Statements	Relevant Controls
3.9.c	It is recommended that Components pursue *Type Security Authorization Process* for information resources that are under the same direct management control; have the same function or mission objective, operating characteristics, security needs, and that reside in the same general operating environment, or in the case of a distributed system, reside in various locations with similar operating environments. *Type Security Authorization Process* shall consist of a master *Security Authorization Process* package describing the common controls implemented across sites and site-specific controls and unique requirements that have been implemented at the individual sites.	---
3.9.d	The AO for a system shall be identified in Trusted Agent FISMA (TAF). The Component CIO shall serve as the AO whenever the System Owner or an appropriate program official has not been named as the AO.	---
3.9.e	Component CISOs shall ensure that all information systems are formally assessed through a comprehensive evaluation of their management, operational, and technical security controls.	CA-2, PM-10
3.9.f	As part of the authorization process, a supporting assessment shall determine the extent to which a particular design and implementation plan meets the DHS required set of security controls.	PM-10
3.9.g	Component CISOs/ISSMs shall ensure that a risk assessment is conducted whenever modifications are made to sensitive information systems, networks, or their physical environments, interfaces, or user community. SPs shall be updated and re-authorized if warranted.	PM-9, RA-3
3.9.h	Components shall authorize systems at Initial Operating Capability (IOC) and every three (3) years thereafter, or whenever a major change occurs, whichever occurs first. An Authority to Operate (ATO) of six (6) months or less shall receive an ATO authorization period waiver from the DHS CISO before submission to the AO for a final authorization decision.	CA-6, PM-10
3.9.i	AOs may grant an Interim Authorization to Operate (IATO) for systems that are undergoing development testing or are in a prototype phase of development. A system shall be assessed and authorized in an ATO letter prior to passing the Acquisition Decision Event 2C milestone in the SELC. IATOs shall not be used for operational systems. The AO may grant an IATO for a maximum period of 6 (six) months and may grant 1 (one) 6 (six) month extension. Systems under an IATO shall not process sensitive information but may attach to system networks for testing.	PL-1, PM-10
3.9.j	If the system is not fully authorized and has not received a full ATO by the end of the second and final IATO, the system shall not be deployed as an operational system.	PL-1, PM-10

Policy ID	DHS Policy Statements	Relevant Controls
3.9.k	Components shall request concurrence from the DHS CISO for all authorizations for 6 (six) months or less.	---
3.9.l	The DHS CISO shall specify tools, techniques, and methodologies used to assess and authorize DHS information systems, report and manage FISMA data, and document and maintain POA&Ms.	CA-1, PM-4
3.9.m	Currently, all DHS systems shall be authorized using the automated tools, TAF and Risk Management System (RMS), which have been approved by the DHS CISO.	CA-1, CA-2, PM-10
3.9.n	The DHS CISO shall maintain a repository for all Security Authorization Process documentation and modifications.	CA-1
3.9.o	Component CISOs shall establish processes to ensure that the Security Authorization Process is used consistently for all Component systems.	CA-1, PM-10
3.9.p	System Owners shall use the POA&M process to manage vulnerabilities, correct deficiencies in security controls, and remediate weaknesses in SPs.	CA-5, PM-4
3.9.q	The AO shall formally assume responsibility for operating an information system at an acceptable level of risk. System operation with sensitive information is prohibited without an ATO.	CA-6, PM-10
3.9.r	ATOs shall only be provided for systems that fully comply with policy or have been granted appropriate exceptions or waivers.	CA-6, PM-10
3.9.s	Artifacts in support of *new* ATOs shall not be older than 13 months. Older artifacts remain valid during the life of a current ATO.	---
3.9.t	The DHS CIO may revoke the ATO of any DHS information system.	CA-6
3.9.u	The Component CIO may revoke the ATO of any Component-level information system.	CA-6
3.9.v	Components shall assign a common control provider to share controls between systems (e.g., at hosting centers). The authorization package of those common controls must be shared with those operating under the controls.	---
3.9.w	DHS enterprise services shall be required to provide a catalog of common controls that have been assessed and authorized by the AO of that service.	---
3.9.x	An Enterprise System Security Agreement (ESSA) shall be developed for all enterprise services.	---

3.10 Information Security Review and Assistance

Policy ID	DHS Policy Statements	Relevant Controls
3.10.a	Components shall submit their information security policies to the DHS CISO for review.	PL-1
3.10.b	Each Component shall establish an information system security review and assistance program within its respective security organization in order to provide System Owners with expert review of programs; to assist in identifying deficiencies; and to provide recommendations for bringing systems into compliance.	CA-7, PL-1, PM-10
3.10.c	Components shall conduct their reviews in accordance with both FIPS 200 and NIST SP 800-53, for specification of security controls. NIST SP 800-53A shall be used for assessing the effectiveness of security controls and for quarterly and annual FISMA reporting.	CA-7, PL-1
3.10.d	The DHS CISO shall conduct information security review and assistance visits across the Department in order to monitor the effectiveness of Component security programs.	CA-2

3.11 Security Working Groups and Forums

Working groups and other forums representing various functional security areas convene on a regular basis.

3.11.1 CISO Council

The CISO Council is the management team responsible for developing and implementing the DHS Information Security Program. The Council is responsible for implementing a security program that meets DHS mission requirements, and also for reviewing specific topic areas assigned by the DHS CIO or the DHS CISO.

The CISO Council is also responsible for establishing and implementing significant security responsibilities; promoting communications between security programs; implementing information systems security acquisition requirements; and developing security best practices in all enterprise and Component information security programs.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.1.a	Component CISOs shall actively participate in the CISO Council.	PL-1, PM-11
3.11.1.b	Members of the CISO Council shall ensure that the DHS CISO is kept apprised of all matters pertinent to the security of information systems.	PL-1, PM-11
3.11.1.c	Members of the CISO Council shall ensure that security-related decisions and information, including updates to the 4300 series of security publications, are	PL-1, PM-11

Policy ID	DHS Policy Statements	Relevant Controls
	distributed to the ISSOs and other appropriate persons.	

Note: Periodically, the CISO Council shall be convened to include Component ISSMs.

3.11.2 DHS Information Security Training Working Group

The DHS Information Security Training Working Group is established to promote collaboration on information security training efforts throughout the Department and to share information on Component-developed training activities, methods, and tools, thereby reducing costs and avoiding duplication of effort. The Information Security Training Working Group is chaired by the DHS Program Director for Information Security Training.

Policy ID	DHS Policy Statements	Relevant Controls
3.11.2.a	Each Component shall appoint a representative to the DHS Information Security Training Working Group.	---
3.11.2.b	Component representatives shall actively participate in the DHS Information Security Training Working Group.	---
3.11.2.c	Components shall abide by the security training requirements listed in the Information Security Awareness, Training, and Education section of this policy.	---

3.12 Information Security Policy Violation and Disciplinary Action

Individual accountability is a cornerstone of an effective security policy. Component Heads are responsible for taking corrective actions whenever security incidents or violations occur and for holding personnel accountable for intentional violations. Each Component must determine how to best address each individual case.

Policy ID	DHS Policy Statements	Relevant Controls
3.12.a	Violations related to information security are addressed in *Standards of Ethical Conduct for Employees of the Executive Branch*; DHS employees may be subject to disciplinary action for failure to comply with DHS security policy whether or not the failure results in criminal prosecution.	PS-8
3.12.b	Non-DHS Federal employees, contractors, or others working on behalf of DHS who fail to comply with Department security policies are subject to termination of their access to DHS systems and facilities whether or not the failure results in criminal prosecution.	PS-8
3.12.c	Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions.	PS-8

3.13 Required Reporting

FISMA requires that the status of the DHS Information Security Program be reported to the OMB on a recurring basis.

Policy ID	DHS Policy Statements	Relevant Controls
3.13.a	Components shall collect and submit quarterly and annual information security program status data as required by FISMA.	CA-2
3.13.b	Components shall use the automated tool approved by the DHS CISO for report generation.	CA-2

3.14 Privacy and Data Security

The DHS Privacy Office is responsible for privacy compliance across the Department, including assuring that technologies used by the Department sustain and do not erode privacy protections relating to the use of personal and Departmental information. The DHS Chief Privacy Officer has exclusive jurisdiction over the development of policy relating to Personally Identifiable Information (PII). Questions concerning privacy-related policy should be directed to the Component Privacy Office or Privacy Point of Contact (PPOC). If the Component does not have a Privacy Office or PPOC, then please contact the DHS Privacy Office (privacy@dhs.gov; 703-235-0780) or refer to the DHS Chief Privacy Officer Web page for additional information.

3.14.1 Personally Identifiable Information

Various regulations place restrictions on the Government's collection, use, maintenance, and release of information about individuals. Regulations require agencies to protect PII, which is any information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to that individual regardless of whether or not the individual is a U.S. citizen, lawful permanent resident, visitor to the U.S., or Department employee or contractor.

Sensitive PII is PII which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of Sensitive PII include Social Security numbers, Alien Registration Numbers (A-number), medical information, and criminal history. The sensitivity of this data requires that stricter handling guidelines be applied. For more information on handling Sensitive PII see: *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security.*

Additional PII and Sensitive PII-related policies are included in the following sections of the DHS 4300A *Sensitive Systems Handbook.*

- Section 3.9, Security Authorization Process, and Security Control Assessments – For Privacy Sensitive Systems, the confidentiality security objective shall be assigned an impact level of at least moderate.

- Section 4.8.2, Laptop Computers and Other Mobile Computing Devices – All information stored on any laptop computer or other mobile computing device is to be encrypted using mechanisms that comply with Section 5.5, Encryption, of this policy.
- Section 5.2.2, Automatic Session Termination – Sessions on workstations and on laptop computers and other mobile computing devices are to be terminated after twenty (20) minutes of inactivity.
- Section 5.3, Auditing – DHS defines computer-readable data extracts as "any Federal record or collection of records containing sensitive PII that is retrieved from a DHS-owned database, through a query, reporting tool, extract generation tool, or other means that is then saved into removable media and/or a separate computer-readable device or application such as another database, a spreadsheet, or a text file." (Attachment S1, *DHS 4300A Sensitive Systems Handbook*).
- Section 5.4.1, Remote Access and Dial-in – Remote access of PII must be approved by the AO. Strong authentication via virtual private network (VPN) or equivalent encryption (e.g., https) and two-factor authentication is required. DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Restrictions are placed on the downloading and remote storage of PII accessed remotely, as noted below in this document.
- Attachment S, "Compliance Framework for Privacy Systems.

The DHS Privacy Office works with Component Privacy Officers, PPOCs, Program Managers, System Owners, and information systems security personnel to ensure that sound privacy practices and controls are integrated into the Department's operations. The DHS Privacy Office implements three types of documents for managing privacy practices and controls for information systems:

- A Privacy Threshold Analysis (PTA) provides a high level description of an information system including the information it contains and how it is used. The PTA is used to determine and document whether or not a PIA and/or SORN are required.
- A Privacy Impact Assessment (PIA) is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared.
- A System of Records Notice (SORN) describes the categories of records within a system of records and describes the routine uses of the data and how individuals can gain access to records and correct errors.

To promote privacy compliance within the Department, the Office has published official Department guidance regarding the requirements and content for PTAs, PIAs, and SORNs. Privacy Compliance Guidance can be found on the DHS Privacy Office website at www.dhs.gov/privacy.

3.14.2 Privacy Threshold Analyses

The PTA provides a high-level description of the system, including the information it contains and how it is used. PTAs are required whenever a new information system is being developed or

an existing system is significantly modified. System Owners and Program Managers are responsible for writing the PTA as part of the SELC process. The Component Privacy Officer or PPOC reviews the PTA and forwards it to the DHS Privacy Office, who determines whether a PIA and/or SORN are required. PTA artifacts expire after three (3) years. DHS MD 0470.2 defines the PTA requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.2.a	A PTA shall be conducted as part of new information system development or whenever an existing system is significantly modified. PTA artifacts expire after three (3) years and a new PTA must be submitted.	PL-5
3.14.2.b	A PTA shall be conducted whenever an information system undergoes security authorization.	---
3.14.2.c	The DHS Chief Privacy Officer shall evaluate the PTA and determine if it is a Privacy Sensitive System and if the system requires a PIA and SORN.	PL-5
3.14.2.d	Information systems shall not be designated operational until the DHS Privacy Office approves the PTA.	PL-5
3.14.2.e	For Privacy Sensitive Systems, the **confidentiality** security objective shall be assigned an impact level of moderate or higher.	RA-2

3.14.3 Privacy Impact Assessments

A PIA is a publicly released assessment of the privacy impact of an information system and includes an analysis of the PII that is collected, stored, and shared. PIAs are required (as determined by the PTA) whenever a new information system is being developed or an existing system is significantly modified. PIAs are the responsibility of the System Owner and the Program Manager as part of the SELC process. OMB Memorandum M-03-22, DHS MD 0470.1, and the *Official DHS Privacy Impact Assessment Guidance* discuss the requirements for conducting PIAs at DHS.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.3.a	PIAs are required (as determined by the PTA) as part of new information system development or whenever an existing system is significantly modified.	PL-5
3.14.3.b	Information systems for which the DHS Privacy Office requires a PIA (as determined by the PTA) shall not be designated operational until the DHS Privacy Office approves the PIA for that system.	PL-5

3.14.4 System of Records Notices

The Privacy Act of 1974 requires a SORN when PII is maintained by a Federal agency in a system of records and the PII is retrieved by a personal identifier. A system of records is "*a*

group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual"[5]. The SORN describes the categories of records and individuals in the system of record; the routine uses of the data; how individuals can gain access to records pertaining to them and correct errors. The term "system of records" is not synonymous with "information system" and can include paper as well as electronic records. SORNs can be written to cover the records in a single group of records or a single information system or they can be written to cover multiple groups of records or multiple information systems.

Information systems that are considered a system of record may not be designated operational until a SORN has been published in the *Federal Register* for thirty days. OMB has issued the benchmark references for development of SORNs: *Privacy Act Implementation, Guidelines and Responsibilities*, July 9, 1975; *Circular A-130,* including Appendix I, "DHS MD 0470.2; and *Official DHS Guidance on System of Records and System of Records Notices.*

OMB requires each SORN to be reviewed every two (2) years to ensure that it accurately describes the system of records. This process is called the Biennial SORN Review Process. The DHS Privacy Office works with Components to ensure that SORN reviews are conducted every two (2) years following publication in the Federal Register.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.4.a	A SORN is required when PII is maintained by a Federal agency in a system of records where information about an individual is retrieved by a unique personal identifier.	---
3.14.4.b	Information systems containing PII shall not be designated operational until a SORN has been published in the Federal Register for thirty (30) days.	CA-6
3.14.4.c	Components shall review and republish SORNs every two (2) years as required by OMB A-130.	---

3.14.5 Protecting Privacy Sensitive Systems

OMB M-06-16, *Protection of Sensitive Agency Information* requires that agencies protect PII that is physically removed from Department locations or is accessed remotely. Physical removal includes both removable media and media in mobile devices (e.g., laptop hard drives). Please refer to the following documents for additional information and policies on protecting PII and Sensitive PII at DHS:

- *Handbook for Safeguarding Sensitive Personally Identifiable Information at the Department of Homeland Security*:
- *DHS 4300A, Sensitive System Handbook, Attachment S*: "Compliance Framework for Privacy Sensitive Systems"

[5] *5 U.S.C. §552a(a)(5) Italics added.*

- *DHS 4300A Sensitive Systems Handbook*, Attachment S1: "Policy and Procedures for Managing Computer-Readable Extracts Containing Sensitive PII."

In addition, see Section 5.3 for PII auditing requirements and Section 5.4.1 for remote access requirements.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.5.a	PII and Sensitive PII removed from a DHS facility on removable media or equipment, such as CDs, DVDs, laptops, PDAs, shall be encrypted unless the information is being sent to an individual as part of a Privacy Act or Freedom of Information Act (FOIA) request.	MP-5 SC-13
3.14.5.b	If PII and Sensitive PII can be physically removed from an information system (e.g., printouts, CDs), the Security Plan (SP) shall document the specific procedures, training, and accountability measures in place to ensure that remote use of the data does not bypass the protections provided by the encryption.	MP-5
3.14.5.c	Systems that as part of routine business remove Sensitive PII in the form of a Computer-Readable Extract (CRE), for example routine system-to-system transmissions of data (routine CREs) shall address associated risks in the system SP.	MP-5
3.14.5.d	Sensitive PII contained within a non-routine or ad hoc CRE (e.g., CREs not included within the boundaries of a source system's security plan) shall not be removed, physically or otherwise, from a DHS facility without written authorization from the Data Owner responsible for ensuring that disclosure of the CRE data is lawful and in compliance with this Policy Directive and with applicable DHS privacy and security policies.	---
3.14.5.e	All ad hoc CREs must be documented, tracked, and validated every ninety (90) days after their creation to ensure that their continued authorized use is still required or that they have been appropriately destroyed or erased.	---
3.14.5.f	Ad hoc CREs shall be destroyed or erased within ninety (90) days unless the information included in the extracts is required beyond that period. Permanent erasure of the extracts or the need for continued use of the data shall be documented by the Data Owner and audited periodically by the Component Privacy Officer or PPOC.	---

3.14.6 Privacy Incident Reporting

The DHS Privacy Office is responsible for implementing the Department's privacy incident response program based on requirements outlined in OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007. Through close collaboration, the DHS Chief Privacy Officer, the DHS CIO, the DHS CISO, the DHS EOC, and Components must ensure that all DHS privacy and computer security incidents are identified, reported, and appropriately responded to, in order to mitigate harm to DHS-

maintained assets, information, and personnel. Incidents involving (or that may involve) PII are subject to strict reporting standards and timelines.

Policy ID	DHS Policy Statements	Relevant Controls
3.14.6.a	Any Component discovering a suspected or confirmed privacy incident shall coordinate with the Component Privacy Officer or PPOC and Component CISO/ISSM to evaluate and subsequently report the incident to the DHS EOC immediately upon discovery. The DHS EOC will then transmit the report to the United States Computer Emergency Readiness Team (US-CERT) within one (1) hour.	IR-4
3.14.6.b	The Component Privacy Officer or PPOC, in cooperation with the Component CISO/ISSM, shall jointly evaluate the incident, but the Component CISO/ISSM is responsible for reporting the incident to the Component SOC or Computer Security Incident Response Capability (CSIRC), or directly to the DHS EOC/CSIRC if the Component does not have its own SOC or CSIRC).	IR-4
3.14.6.c	For Components without Privacy Officers or PPOCs, the Component CISO/ISSM shall report *all* types of privacy incidents, whether or not they involve information resources. This unitary reporting process shall remain in effect until each Component has a Privacy Officer or PPOC who can fulfill the reporting duties.	IR-6
3.14.6.d	DHS personnel shall also report suspected or confirmed privacy incidents to their Program Manager immediately upon discovery/detection, regardless of the manner in which it might have occurred.	IR-6
3.14.6.e	Components shall follow the *DHS Privacy Incident Handling Guide*.	---

3.14.7 E-Authentication

Identity verification or authentication (e-authentication) is needed to ensure that online Government services are secure and that individual privacy is protected. Each DHS system must be evaluated to determine whether e-authentication requirements apply. Only federated identity providers approved through the Federal CIO Council's Identity, Credentialing, and Access Management's (ICAM) Trust Framework Provider Adoption Process (TFPAP) should be used. Components should see www.IDmanagement.gov for details regarding the Federal Identity, Credentialing, and Access Management (FICAM) initiative.

E-authentication guidance is provided in the following:

- OMB M-0404, *E-Authentication Guidance for Federal Agencies*
- NIST SP 800-63, *Electronic Authentication Guideline*

Policy ID	DHS Policy Statements	Relevant Controls
3.14.7.a	For systems that allow online transactions, Components shall determine whether e-authentication requirements apply.	IA-2
3.14.7.b	Components shall determine the appropriate assurance level for e-authentication by following the steps described in OMB M-04-04, *E-Authentication Guidance for Federal Agencies*.	IA-2
3.14.7.c	Components shall implement the technical requirements described in NIST SP 800-63, *Electronic Authentication Guideline*, at the appropriate assurance level for those systems with e-authentication requirements.	IA-2
3.14.7.d	Components shall ensure that each SP reflects the e-authentication status of the respective system.	IA-2, PL-2
3.14.7.e	Programs considering the use of e-authentication are required to consult their privacy officer to determine whether a change is significant enough to warrant a new or updated PTA, thus initiating the review of privacy risks and how they will be mitigated.	PL-5
3.14.7.f	Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines.	---
3.14.7.g	All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational.	---
3.14.7.h	All new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials.	---

3.15 DHS CFO Designated Systems

DHS CFO Designated Systems are systems that require additional management accountability to ensure effective internal control exists over financial reporting. The DHS CFO publishes the approved list of CFO Designated Systems annually. This section provides additional requirements for these systems based on Appendix A to OMB Circular A-123, *Management's Responsibility for Internal Control*. The requirements contained in OMB Circular A-123 have been mapped to the NIST SP 800-53 controls and documented in Attachment R, *Compliance Framework for CFO-Designated Financial Systems* to *DHS 4300A Sensitive Systems Handbook*. These requirements are in addition to both the other security requirements established in this Policy Directive and other CFO-developed financial system Line of Business requirements.

Wherever there is a conflict between this section and other sections of this Policy Directive regarding requirements for CFO Designated Systems, this section shall take precedence.

These additional requirements provide a strengthened assessment process and form the basis for management's assurance of internal control over financial reporting. The strengthened process requires management to document the design and test the operating effectiveness of controls for CFO Designated Systems. The system owner is responsible for ensuring that all requirements,

including security requirements, are implemented on DHS systems. Component CISOs/ISSMs must coordinate with their CFO organization to ensure that these requirements are implemented.

Policy ID	DHS Policy Statements	Relevant Controls
3.15.a	System owners are responsible for ensuring that security control assessments of key security controls (i.e., Security Control Assessment and Security Assessment Report [SAR]) for CFO Designated Systems are completed annually in TAF. This includes updating the security control assessment & SAR annually.	CA-2, CA-7
3.15.b	The DHS CFO shall designate the systems that must comply with additional internal controls and the Office of the CFO shall review and publish this list annually.	CA-2
3.15.c	Component CISOs/ISSMs shall ensure that vulnerability assessments and verification of critical patch installations are conducted on all CFO Designated Systems. Vulnerability assessment shall be performed at least annually.	RA-5
3.15.d	All CFO Designated Systems shall be assigned a minimum impact level of "moderate" for confidentiality, integrity, and availability. If warranted by a risk based assessment, the integrity objective shall be elevated to "high."	RA-2
3.15.e	All Component security authorizations for CFO Designated Systems shall be approved and signed by the Component CFO.	CA-6
3.15.f	System Owners shall ensure that Contingency plans are created for *all* CFO Designated Systems requiring moderate availability and Disaster Recovery plans are created for *all* CFO Designated Systems requiring high availability and that each plan is tested annually.	CP-2, CP-4
3.15.g	Component CISOs/ISSMs shall ensure that weekly incident response tracking is performed for all of their respective CFO Designated Systems.	IR-5
3.15.h	Component CISOs/ISSMs shall ensure that incidents related to their respective CFO Designated Systems are reported to the Component CFO.	IR-4, IR-6
3.15.i	The SP shall be updated for CFO Designated Systems at least annually. Key controls prescribed in Attachment R, *Compliance Framework for CFO Designated Systems* shall be identified in the SP.	PL-2
3.15.j	Component CISOs/ISSMs must request a waiver or exception from the DHS CISO if a key control weakness is identified for a CFO Designated System and not remediated within twelve (12) months.	CA-5, CA-7
3.15.k	Component CFOs shall ensure that a fulltime dedicated ISSO is assigned to each CFO Designated System. CFO Designated System ISSOs may be assigned to more than one CFO Designated System.	---

Policy ID	DHS Policy Statements	Relevant Controls
3.15.l	CFO Designated System ATOs shall be rescinded if Components fail to comply with testing and reporting requirements established within this policy.	CA-1, CA-6
3.15.m	Component CFOs shall work with their Component CISOs/ISSMs to approve any major system changes to CFO Designated Systems identified in the DHS inventory.	CA-1, CM-8

3.16 Social Media

Social Media hosts are public content sharing websites that allow individual users to upload, view, and share content such as video clips, press releases, opinions and other information. The DHS Office of Public Affairs (OPA) will publish Terms of Service (TOS) and guidelines for posting to these sites. In some cases the Department will develop its own TOS, and in other cases it will endorse those of other Federal agencies such as the General Services Administration (GSA) or Office of Personnel Management (OPM). Due to the high threat of malware, Social Media host sites have been blocked at the Trusted Internet Connection (TIC).

Policy ID	DHS Policy Statements	Relevant Controls
3.16.a	Only OPA-designated content managers (Department level and Component level) may post content, and only those individuals designated by OPA for this purpose shall be granted access on a continuing basis.	SA-6
3.16.b	Posted content shall be in keeping with the Department's Terms of Service (TOS) and guidelines for a given social media host (e.g., YouTube, Twitter). This condition is also met if the Department endorses another appropriate Federal agency's guidance or TOS (e.g., GSA, OPM). Under no circumstances shall sensitive information be posted to social media sites.	---
3.16.c	Content shall not be posted to any social media site for which the Department has not approved and published *both* final posting guidelines *and* TOS.	SA-6
3.16.d	Content managers shall review and understand the appropriate Department-level TOS for the appropriate social media host.	---
3.16.e	Content managers shall make a risk decision prior to posting any information and shall recognize that social medial hosts are not DHS information systems and therefore subject only to the DHS TOS and not to DHS policy. Once released, information is no longer under DHS control.	---

There are a number of security technologies that are especially important to consider when dealing with social media issues. These include:

- Trusted Internet Connections (TIC) – Section 5.4.4
- Host Configuration and Hardening – Section 4.8.4

- Enterprise Operations Center (EOC) and Network Operations Center (NOC) – Section 4.9
- Two-Factor Authentication – Section 5.4.1
- Domain Name System Security Extensions (DNSSEC) Capabilities – Section 5.4.3
- Trust Zones – Section 5.4.3
- Signed Code – Section 5.4.5
- Patching and Anti-Virus – Section 5.6

3.17 Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act of 1996 (HIPAA)[6] addresses the privacy of individuals' health information by establishing a Federal privacy standard for health information and how it can be used and disclosed.

HIPAA prohibits the use or disclosure without the authorization of the individual or as part of an exception contained in HIPAA of Protected Health Information (PHI), electronic or otherwise, for any purpose other than treatment, payment, or health care operations for that individual.

Because of the diverse mission of DHS, it may be necessary for some Components to collect PHI as part of a larger mission requirement (for example detainee processing, disaster relief, etc.). This section applies to all Components and personnel who collect, process, or store PHI (refer to NIST SP 800-66 for further information).

Policy ID	DHS Policy Statements	Relevant Controls
3.17.a	Components whose systems collect, process, or store Protected Health Information (PHI) shall ensure that the stored information is appropriately protected in compliance with HIPAA and that access or disclosure is limited to the minimum required.	---
3.17.b	Affected Components shall work with the DHS Privacy Office, Component Privacy Office, or PPOC to ensure that privacy and disclosure policies comply with HIPAA requirements.	---
3.17.c	Affected Components shall ensure that employees with access to DHS systems that collect, process, or store PHI are trained in HIPAA requirements.	---
3.17.d	Affected Components shall establish administrative processes for responding to complaints; requesting corrections to health information; and tracking of PHI disclosures.	---
3.17.e	When collecting PHI, Components shall issue a privacy notice to individuals concerning the use and disclosure of their PHI.	---

[6] *Public Law 104-191*

4.0 OPERATIONAL POLICIES

4.1 Personnel

Department of Homeland Security (DHS) systems face threats from a myriad of sources. The intentional and unintentional actions of system users can potentially harm or disrupt DHS systems and facilities and could result in destruction or modification of the data being processed, denial of service, and unauthorized disclosure of data. It is thus highly important that stringent safeguards be in place to reduce the risk associated with these types of threats.

4.1.1 Citizenship, Personnel Screening, and Position Categorization

Policy ID	DHS Policy Statements	Relevant Controls
4.1.1.a	Components shall designate the position sensitivity level for all Government and contractor positions that use, develop, operate, or maintain information systems and shall determine risk levels for each contractor position. Position sensitivity levels shall be reviewed annually and revised as appropriate.	PS-2, PS-3, PS-7
4.1.1.b	Components shall ensure that the incumbents of these positions have favorably adjudicated background investigations commensurate with the defined position sensitivity levels.	PS-2, PS-3, PS-7
4.1.1.c	Components shall ensure that no Federal employee is granted access to any DHS system without having a favorably adjudicated Minimum Background Investigation (MBI) as defined in DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, Chapter 2, Federal Employee/Applicant Suitability Requirements. In cases where non-DHS Federal employees have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 2, paragraph G). Active duty United States Coast Guard (USCG) and other personnel subject to the Uniform Code of Military Justice shall be exempt from this requirement.	PS-3
4.1.1.d	Components shall ensure that no contractor personnel are granted access to DHS systems without having a favorably adjudicated Background Investigation (BI) as defined in Department of Homeland Security Acquisition Regulation (HSAR) and the DHS Instruction 121-01-007, *Personnel Suitability and Security Program*, Chapter 3, Excepted Service Federal Employee and Contractor Employee Fitness Requirements. In cases where contractor personnel have been investigated by another Federal agency, DHS Component personnel security organizations may, whenever practicable, use these investigations to reduce investigation requests, associated costs, and unnecessary delays (Chapter 3, paragraph G).	PS-3
4.1.1.e	Components shall ensure that only U.S. Citizens are granted access to DHS systems and networks. Exceptions to the U.S. Citizenship requirement may be granted by the Component Head or designee with the concurrence of the	PS-3

Policy ID	DHS Policy Statements	Relevant Controls
	Office of Security and the DHS Chief Information Officer (CIO), in accordance with Section 1.5.4, of this policy, "Requests for Exception to U.S. Citizenship Requirement."	

4.1.2 Rules of Behavior

Policy ID	DHS Policy Statements	Relevant Controls
4.1.2.a	Components shall ensure that rules of behavior contain acknowledgement that the user has no expectation of privacy (a "Consent to Monitor" provision) and that disciplinary actions may result from violations.	PL-4
4.1.2.b	Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data.	AT-1, AT-2, PL-4

4.1.3 Access to Sensitive Information

Policy ID	DHS Policy Statements	Relevant Controls
4.1.3.a	System Owners shall ensure that users of the information systems supporting their programs have a valid requirement to access these systems.	AC-2

4.1.4 Separation of Duties

Separation of duties is intended to prevent a single individual from being able to disrupt or corrupt a critical security process.

Policy ID	DHS Policy Statements	Relevant Controls
4.1.4.a	Components shall divide and separate duties and responsibilities of critical information system functions among different individuals to minimize the possibility of any one individual having the necessary authority or system access to be able to engage in fraudulent or criminal activity.	AC-2, AC-5
4.1.4.b	All individuals requiring administrator privileges shall be reviewed and approved by the appropriate Authorizing Official (AO). The AO may delegate this duty to the appropriate system owner or Program Manager.	AC-2
4.1.4.c	Individuals requiring administrator privileges shall be assigned administrator accounts separate from their normal user accounts.	AC-6
4.1.4.d	Administrator accounts shall be used only for performing required administrator duties. Individuals shall use their regular user accounts to	AC-6

Policy ID	DHS Policy Statements	Relevant Controls
	perform all other functions not directly tied to administrator duties (checking email, accessing the Internet).	

4.1.5 Information Security Awareness, Training, and Education

Policy ID	DHS Policy Statements	Relevant Controls
4.1.5.a	Components shall establish an information security training program for users of DHS information systems.	AT-1
4.1.5.b	DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) accessing DHS systems shall receive initial training and annual refresher training in security awareness and accepted security practices. Personnel shall complete security awareness training within twenty-four (24) hours of being granted a user account. If a user fails to meet this training requirement, user access shall be suspended.	AT-1, AT-4
4.1.5.c	DHS personnel, contractors, or others working on behalf of DHS (i.e. employees, detailees, military) with significant security responsibilities (e.g., Information Systems Security Officers (ISSO), system administrators) shall receive initial specialized training and thereafter annual refresher training specific to their security responsibilities.	AT-3
4.1.5.d	Components shall maintain awareness training records to include: Component name, name of trainee, training course title, type of training received, and completion date of training.	AT-4
4.1.5.e	Components shall maintain role-based training records to include Component name, name of trainee, security role of trainee, training course title, type of training received, completion date of training, and cost of training.	AT-4
4.1.5.f	User accounts and access privileges, including access to email, shall be disabled for those DHS employees who have not received annual refresher training, unless a waiver is granted by the Component's Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM).	AT-1
4.1.5.g	Components shall prepare and submit an annual security awareness and role-based training plan, as specified by the DHS Information Security Training Program Office.	AT-1
4.1.5.h	Components shall prepare and submit information security awareness reports with content, frequency, format, and distribution at the request of the DHS CISO.	AT-1
4.1.5.i	Components shall at the request of the DHS Information Security Training Program Office provide evidence of training by submitting copies of training	AT-4

Policy ID	DHS Policy Statements	Relevant Controls
	schedules, training rosters, and training reports.	
4.1.5.j	The DHS CISO shall review Component information security awareness and role-based training programs annually.	AT-1
4.1.5.k	Components shall submit a roster the during the first month and during the seventh month of each fiscal year identifying all significant information security personnel, including full name, security role, employment status (federal employee, military, contractor), and work location (state). At a minimum, the roster will include all standard information security roles: Chief Information Officer, Chief Information Security Officer, Authorizing Official, Program Manager, System Owner, Information System Security Officer, Security Operations Center Manager, System Administrator (Windows-based), and Contracting Officer/Contracting Officer Technical Representative.	AT-3

4.1.6 Separation from Duty

Policy ID	DHS Policy Statements	Relevant Controls
4.1.6.a	Components shall implement procedures to ensure that system access is revoked for DHS employees, contractors, or others working on behalf of DHS who leave the Component, are reassigned to other duties, or no longer require access.	AC-2
4.1.6.b	Components shall establish procedures to ensure that all DHS property and assets related to information systems are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual.	PS-4
4.1.6.c	Accounts for personnel on extended absences shall be temporarily suspended.	AC-2
4.1.6.d	System Owners shall review information system accounts supporting their programs at least annually.	AC-2

4.2 Physical Security

4.2.1 General Physical Access

Policy ID	DHS Policy Statements	Relevant Controls
4.2.1.a	Access to DHS buildings, rooms, work areas, spaces, and structures housing information systems, equipment, and data shall be limited to authorized personnel.	PE-2
4.2.1.b	Controls for deterring, detecting, restricting, and regulating access to sensitive	PE-3

Policy ID	DHS Policy Statements	Relevant Controls
	areas shall be in place and shall be sufficient to safeguard against possible loss, theft, destruction, damage, hazardous conditions, fire, malicious actions, and natural disasters.	
4.2.1.c	Controls shall be based on the level of classification and risk, determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9
4.2.1.d	Visitors shall sign in upon entering DHS facilities that house information systems, equipment, and data. They shall be escorted during their stay and sign out upon leaving. Access by non-DHS contractors or vendors shall be limited to those work areas requiring their presence. Visitor logs shall be maintained and available for review for one (1) year.	PE-7
4.2.1.e	These requirements shall extend to DHS assets located at non-DHS facilities or non-DHS assets and equipment that host DHS data.	---

4.2.2 Sensitive Facility

Policy ID	DHS Policy Statements	Relevant Controls
4.2.2.a	Facilities processing, transmitting, or storing sensitive information shall incorporate physical protection measures based on the level of risk. The risk shall be determined in accordance with Departmental security policy as reflected in this and other relevant documents.	PE-1, PM-9

4.3 Media Controls

4.3.1 Media Protection

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.a	Components shall ensure that all media containing sensitive information, including hard copy media, backup media, and removable media such as USB drives, are stored when not in use in a secure location (e.g., a locked office, room, desk, bookcase, file cabinet, locked tape device, or in other storage that prohibits access by unauthorized persons).	MP-2, MP-4, PE-1
4.3.1.b	Components shall ensure that all offsite backup media are protected as per guidance in this section.	CP-6
4.3.1.c	DHS personnel, contractors, and others working on behalf of DHS are prohibited from using any non-Government-issued removable media (USB drives, in particular) and from connecting them to DHS equipment or networks or using them to store DHS sensitive information.	MP-2

Policy ID	DHS Policy Statements	Relevant Controls
4.3.1.d	Systems requiring encryption shall comply with Section 5.5.1, Encryption, of this Policy Directive. DHS-owned USB drives shall use encryption.	IA-7, SC-13
4.3.1.e	DHS-owned removable media shall not be connected to any non-DHS information system unless the AO has determined that the risk is acceptable based on compensating controls and published acceptable use guidance that has been approved by the respective CISO or Information Systems Security Manager (ISSM). (The respective CISO is the CISO with that system in his or her inventory.)	AC-20, MP-2, PM-9
4.3.1.f	Components shall follow established procedures to ensure that paper and electronic outputs from systems containing sensitive information are protected.	MP-1
4.3.1.g	Users shall ensure proper protection of printed output. Printing of sensitive documents shall occur only when a trusted person is attending the printer.	SI-12
4.3.1.h	Components shall follow the procedures established by DHS Management Directive (MD) 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*, for the transportation or mailing of sensitive media.	MP-5

4.3.2 Media Marking and Transport

Policy ID	DHS Policy Statements	Relevant Controls
4.3.2.a	Media determined by the information owner to contain sensitive information shall be appropriately marked in accordance with DHS MD 11042.1, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information*.	MP-3
4.3.2.b	Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel.	MP-5

4.3.3 Media Sanitization and Disposal

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.a	Components shall ensure that any information systems storage medium containing sensitive information is sanitized using approved sanitization methods before it is disposed of, reused, recycled, or returned to the owner or manufacturer.	MP-6
4.3.3.b	Components shall maintain records of the sanitization and disposition of information systems storage media.	MP-6

Policy ID	DHS Policy Statements	Relevant Controls
4.3.3.c	Components shall periodically test degaussing equipment to verify that the equipment is functioning properly.	MP-6

4.3.4 Production, Input/Output Controls

Policy ID	DHS Policy Statements	Relevant Controls
4.3.4.a	Components shall follow established procedures to ensure that sensitive information cannot be accessed or stolen by unauthorized individuals.	SI-12
4.3.4.b	These procedures shall address not only the paper and electronic outputs from systems but also the transportation or mailing of sensitive media.	SI-12

4.4 Voice Communications Security

4.4.1 Private Branch Exchange

Policy ID	DHS Policy Statements	Relevant Controls
4.4.1.a	Components shall provide adequate physical and information security for all DHS-owned Private Branch Exchanges (PBX). (Refer to NIST Special Publication (SP) 800-24, *PBX Vulnerability Analysis*, for guidance on detecting and fixing vulnerabilities in PBX systems.)	CM-2

4.4.2 Telephone Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.4.2.a	Components shall develop guidance for discussing sensitive information over the telephone. Guidance shall be approved by a senior Component official and is subject to review and approval by the DHS CISO. Under no circumstances shall classified national security information be discussed over unsecured telephones.	PL-4

4.4.3 Voice Mail

Policy ID	DHS Policy Statements	Relevant Controls
4.4.3.a	Sensitive information shall not be communicated over nor stored in voice mail.	PL-4

4.5 Data Communications

4.5.1 Telecommunications Protection Techniques

Policy ID	DHS Policy Statements	Relevant Controls
4.5.1.a	Components shall carefully select the telecommunications protection techniques that meet their information security needs in the most cost-effective manner, consistent with Departmental and Component information system security policies. Approved protected network services (PNS) may be used as cost-effective alternatives to the use of encryption for sensitive information requiring telecommunications protection.	CM-2

4.5.2 Facsimiles

Policy ID	DHS Policy Statements	Relevant Controls
4.5.2.a	Components shall implement and enforce technical controls for fax technology and systems (including fax machines, servers, gateways, software, and protocols) that transmit and receive sensitive information.	SC-1, SC-7, SC-8, SC-9
4.5.2.b	Components shall configure fax servers to ensure that incoming lines cannot be used to access the network or any data on the fax server.	AC-4

4.5.3 Video Teleconferencing

Policy ID	DHS Policy Statements	Relevant Controls
4.5.3.a	Components shall implement controls to ensure that only authorized individuals are able to participate in each video conference.	AC-3, PE-3
4.5.3.b	Components shall ensure that appropriate transmission protections, commensurate with the highest sensitivity of information to be discussed, are in place throughout any video teleconference.	SC-8, SC-9
4.5.3.c	Video teleconferencing equipment and software shall be disabled when not in use.	AC-3, PE-3

4.5.4 Voice Over Data Networks

Voice over Internet Protocol (VoIP) and similar technologies move voice over digital networks. These technologies use protocols originally designed for data networking. Such technologies include Voice over Frame Relay, Voice over Asynchronous Transfer Mode, and Voice over Digital Subscriber Line (refer to National Institute of Standards and Technology (NIST) SP 800-58 for further information).

Policy ID	DHS Policy Statements	Relevant Controls
4.5.4.a	Prior to implementing voice over data network technology, Components shall conduct rigorous risk assessments and security testing and provide a business justification for their use. Any systems that employ this technology shall be authorized for this purpose with residual risks clearly identified.	SC-19, PM-9
4.5.4.b	Voice over data network implementations shall have sufficient redundancy to ensure network outages do not result in the loss of both voice and data communications.	SC-19
4.5.4.c	Components shall ensure appropriate identification and authentication controls, audit logging, and integrity controls are implemented on every element of their voice over data networks.	SC-19
4.5.4.d	Components shall ensure that physical access to voice over data network elements is restricted to authorized personnel.	SC-19

4.6 Wireless Network Communications

Wireless network communications technologies include the following:

- Wireless systems (e.g., wireless local area networks [WLAN], wireless wide area networks [WWAN], wireless personal area networks [WPAN], peer-to-peer wireless networks, information systems that leverage commercial wireless services). Wireless systems include the transmission medium, stationary integrated devices, firmware, supporting services, and protocols
- Wireless portable electronic devices (PED) capable of storing, processing, or transmitting sensitive information (e.g., personal digital assistants [PDA], smart telephones, two-way pagers, handheld radios, cellular telephones, personal communications services [PCS] devices, multifunctional wireless devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices)
- Wireless tactical systems, including mission-critical communication systems and devices (e.g., include Land Mobile Radio [LMR] subscriber devices and infrastructure equipment, remote sensors, technical investigative communications systems)
- Radio Frequency Identification (RFID)

Policy ID	DHS Policy Statements	Relevant Controls
4.6.a	Components are prohibited from introducing new wireless network communications technologies into the enterprise unless the appropriate AO specifically approves a technology and application.	AC-18

Policy ID	DHS Policy Statements	Relevant Controls
4.6.b	Components using Public Key Infrastructure (PKI)-based encryption on wireless systems, wireless PEDs, and wireless tactical systems shall implement and maintain a key management plan approved by the DHS PKI Policy Authority.	IA-5, SC-12

4.6.1 Wireless Systems

Wireless system policy and procedures are described more completely in Attachment Q1 (*Wireless Systems*) to the DHS 4300A *Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.1.a	Annual information security assessments shall be conducted on all approved wireless systems. Wireless information security assessments shall enumerate vulnerabilities, risk statements, risk levels, and corrective actions.	CA-2, PM-9
4.6.1.b	A Plan of Action and Milestones (POA&M) shall be developed to address wireless information security vulnerabilities. Plans shall prioritize corrective actions and implementation milestones in accordance with defined risk levels.	CA-5, PM-4, PM-9
4.6.1.c	Components shall identify countermeasures to denial-of-service attacks and complete a risk based evaluation prior to approving the use of a wireless PED	AC-19, PM-9, SC-5
4.6.1.d	SPs shall adopt a defense-in-depth strategy that integrates firewalls, screening routers, wireless intrusion detection systems, antivirus software, encryption, strong authentication, and cryptographic key management to ensure that information security solutions and secure connections to external interfaces are consistently enforced.	SI-3
4.6.1.e	A migration plan shall be implemented for legacy wireless systems that are not compliant with DHS information security policy. The migration plan shall outline the provisions, procedures, and restrictions for transitioning the legacy systems to DHS-compliant security architectures. Operation of these noncompliant systems before and during the migration requires an approved waiver or exception to policy from the DHS CISO.	CA-5
4.6.1.f	Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO annually.	AC-18, PM-5
4.6.1.g	Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems.	AC-18

4.6.2 Wireless Portable Electronic Devices

Wireless PEDs include PDAs, smart telephones, two-way pagers, handheld radios, cellular telephones, PCS devices, multifunctional wireless devices, GPS devices, portable audio/video recording devices with wireless capability, scanning devices, messaging devices, and any other wireless clients capable of storing, processing, or transmitting sensitive information.

Wireless PED policy and procedures are described more completely in *DHS 4300A Sensitive Systems Handbook* Attachment Q2, "Wireless Portable Electronic Devices."

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.a	The use of wireless PEDs and accessory devices in areas where classified information is discussed, maintained, or distributed is prohibited unless specifically authorized in writing by the AO for the system used in the area	AC-19, PL-4
4.6.2.b	Wireless PEDs shall not be tethered or otherwise physically or wirelessly connected to the DHS-wired core network without written consent from the AO.	AC-18, AC-19
4.6.2.c	Wireless PEDs shall not be used to store, process, or transmit combinations, personal identification numbers (PIN), or sensitive information in unencrypted formats.	AC-19, IA-5, IA-7
4.6.2.d	Wireless PEDs such as BlackBerry devices and smart phones shall implement strong authentication, data encryption, and transmission encryption technologies. Portable electronic devices such as BlackBerry devices and smart phones shall be password-protected, with a security timeout period established. For BlackBerry devices, the security timeout shall be set to ten (10) minutes.	AC-19, IA-7, SC-8, SC-9, SC-13
4.6.2.e	SPs shall promulgate the provisions, procedures, and restrictions for using wireless PEDs to download mobile code in an approved manner.	SC-18
4.6.2.f	Wireless PEDs shall be operated only when current DHS TRM-approved versions of antivirus software and software patches are installed.	SI-3
4.6.2.g	Cost-effective countermeasures to denial-of-service attacks shall be identified and established prior to a wireless PED being approved for use.	SC-5 SC-7
4.6.2.h	Components shall maintain a current inventory of all approved wireless PEDs in operation.	PM-5
4.6.2.i	Wireless PEDs shall be sanitized of all information before being reused by another individual, office, or Component within DHS or before they are surplused; wireless PEDs that are being disposed of, recycled, or returned to the owner or manufacturer shall first be sanitized using approved procedures.	MP-6
4.6.2.j	For legacy wireless PEDs that are not compliant with DHS information	CA-5

Policy ID	DHS Policy Statements	Relevant Controls
	security policy a migration plan shall be implemented that outlines the provisions, procedures, and restrictions for transitioning these wireless PEDs to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO.	CA-6
4.6.2.k	Components shall ensure that personally-owned PEDs and Government-owned PEDs not authorized to process classified information are not permitted in conference rooms or secure facilities where classified information is discussed.	AC-19, PE-18
4.6.2.l	The AO shall approve the use of Government-owned PEDs to process, store, or transmit sensitive information.	CA-6
4.6.2.m	The use of add-on devices, such as cameras and recorders, is not authorized unless approved by the AO. Functions that can record or transmit sensitive information via video, Infrared (IR), or Radio Frequency (RF) shall be disabled in areas where sensitive information is discussed.	AC-19, CM-7, PE-18, SC-7

4.6.2.1 Cellular Phones

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.1.a	Components shall develop guidance for discussing sensitive information on cellular phones. Guidance shall be approved by a senior Component official and is subject to review by the DHS CISO. Under no circumstances shall classified information be discussed on cellular phones.	PL-4

4.6.2.2 Pagers

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.2.a	Pagers shall not be used to transmit sensitive information.	PL-4

4.6.2.3 Multifunctional Wireless Devices

Wireless devices have evolved to be multifunctional (cell phones, pagers, and radios can surf the Internet, retrieve email, take and transmit pictures). Most of these functions do not have sufficient security.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.a	Functions that cannot be encrypted using approved cryptographic modules shall not be used to process, store, or transmit sensitive information.	AC-19, SC-8, SC-9, SC-12

Policy ID	DHS Policy Statements	Relevant Controls
4.6.2.3.b	Functions that transmit or receive video, IR, or radio frequency (RF) signals shall be disabled in areas where sensitive information is discussed.	AC-19, PE-18
4.6.2.3.c	Short Message Service (SMS) and Multimedia Messaging Service (MMS) shall not be used to process, store, or transmit sensitive information, and shall be disabled whenever possible.	—

4.6.3 Wireless Tactical Systems

Wireless tactical systems include Land Mobile Radio (LMR) subscriber devices, infrastructure equipment, remote sensors, and technical investigative communications systems. Because they are often deployed under circumstances in which officer safety and mission success are at stake, wireless tactical systems require even greater security measures. To ensure secure tactical communications, Components must implement strong identification, authentication, and encryption protocols designed specifically for each wireless tactical system.

Wireless tactical system policy and procedures are described more completely in Attachment Q3 (*Wireless Tactical Systems*) to the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.a	AOs shall be immediately notified when any security features are disabled in response to time-sensitive, mission-critical incidents.	CM-3
4.6.3.b	Wireless tactical systems shall implement strong identification, authentication, and encryption.	IA-2, IA-7, SC-8, SC-9
4.6.3.c	Cost-effective countermeasures to denial-of-service attacks shall be identified and implemented prior to a wireless tactical system being approved for use.	SC-5
4.6.3.d	Components shall maintain a current inventory of all approved wireless tactical systems in operation.	PM-5
4.6.3.e	A migration plan shall be implemented for legacy tactical wireless systems that are not compliant with DHS information security policy; The migration plan will outline the provisions, procedures, and restrictions for transitioning the legacy systems to DHS-compliant security architectures. Operation of these noncompliant systems requires an approved waiver or exception from the DHS CISO, as appropriate.	---
4.6.3.f	The security configuration of LMR subscriber units shall be validated via over-the-air-rekeying (OTAR) or hard rekey using a crypto-period no longer than 180 days.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
4.6.3.g	All LMR systems shall comply with Project 25 (P25, EIA/TIA-102) security standards where applicable.	CM-2

4.6.4 Radio Frequency Identification

Radio Frequency Identification (RFID) enables wireless identification of objects over significant distances. Because of the computing limitations of RFID tags, it often is not feasible to implement many of the security mechanisms, such as cryptography and strong authentication, that are commonly supported on personal workstations, servers, and network infrastructure devices. RFID security controls can support Departmental and Component privacy objectives, mitigate risks to business processes, and prevent the disclosure of sensitive data.

RFID policy and procedures are described more completely in *"Sensitive RFID Systems,"* Attachment Q4 to the *DHS 4300A Sensitive Systems Handbook*.

Policy ID	DHS Policy Statements	Relevant Controls
4.6.4.a	Components implementing RFID systems shall assess hazards of electromagnetic radiation to fuel, ordnance, and personnel before deployment of the RFID technology.	PE-18
4.6.4.b	Components shall limit data stored on RFID tags to the greatest extent possible, recording information beyond an identifier only when required for the application mission. When data beyond an identifier is stored on a tag, the tag's memory shall be protected by access control.	AC-6, PL-5
4.6.4.c	Components shall develop a contingency plan, such as the use of a fallback identification technology, to implement in case of an RFID security breach or system failure.	---
4.6.4.d	Components shall identify and implement appropriate operational and technical controls to limit unauthorized tracking or targeting of RFID-tagged items when these items are expected to travel outside the Component's physical perimeter.	AC-14
4.6.4.e	When an RFID system is connected to a DHS data network, Components shall implement network security controls to segregate RFID network elements such as RFID readers, middleware, and databases from other non-RFID network hosts.	CM-6
4.6.4.f	Components implementing RFID technology shall determine whether or not tag cloning is a significant business risk. If such a significant risk exists, then tag transactions shall be cryptographically authenticated.	IA-7, PM-9, RA-3

4.7 Overseas Communications

Policy ID	DHS Policy Statements	Relevant Controls
4.7.a	Where required or appropriate, all communications outside of the United States and its territories shall be in accordance with the Department of State Foreign Affairs Manual (FAM), 12 FAM 600, *Information Security Technology*.	---

4.8 Equipment

4.8.1 Workstations

Policy ID	DHS Policy Statements	Relevant Controls
4.8.1.a	Components shall configure workstations to either log off, or activate a password-protected lock, or password-protected screensaver within fifteen (15) minutes of user inactivity.	AC-11, CM-6
4.8.1.b	Components shall ensure that workstations are protected from theft.	PE-3
4.8.1.c	Users shall either log off or lock their workstations when unattended.	---

4.8.2 Laptop Computers and Other Mobile Computing Devices

Policy ID	DHS Policy Statements	Relevant Controls
4.8.2.a	Information stored on any laptop computer or other mobile computing device that may be used in a residence or on travel shall use encryption in accordance with Section 5.5.1, Encryption, for data at rest and in motion. Passwords, tokens and Smart Cards shall not be stored on or with the laptop or other mobile computing device.	AC-19, IA-2, SC-12
4.8.2.b	Laptop computers shall be powered down when not in use (due to volatile memory vulnerabilities).	AC-19, PL-4
4.8.2.c	When unattended, laptop computers and other mobile computing devices shall be secured in locked offices, secured with a locking cable, or in a locked cabinet, or desk.	AC-19, PE-3, PL-4
4.8.2.d	Users shall obtain the written approval of the office director before taking a laptop computer or other mobile computing device outside of the United States or its territories.	AC-19, PL-4

4.8.3 Personally Owned Equipment and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.3.a	Personally owned equipment and software shall not be used to process, access, or store sensitive information without the written prior approval of the AO.	SA-6
4.8.3.b	Equipment that is not owned or leased by the Federal Government, or operated by a contractor on behalf of the Federal Government, shall not be connected to DHS equipment or networks without the written prior approval of the Component CISO/ISSM.	SA-9
4.8.3.c	Any device that has been obtained through civil or criminal asset forfeiture shall not be used as part of a DHS information system nor used to process DHS data.	AC-20

4.8.4 Hardware and Software

Policy ID	DHS Policy Statements	Relevant Controls
4.8.4.a	Components shall ensure that DHS information systems follow the hardening guides for operating systems and the configuration guides for applications promulgated by the DHS CISO. *DHS Sensitive Systems Handbook 4300A*, Enclosure 1, includes the DHS Secure Baseline Configuration Guides.	CM-2, CM-6
4.8.4.b	Components shall limit access to system software and hardware to authorized personnel.	AC-3, CM-5
4.8.4.c	Components shall test, authorize, and approve all new and revised software and hardware prior to implementation in accordance with their Configuration Management Plan.	CM-2, CM-3
4.8.4.d	Components shall manage systems to reduce vulnerabilities through vulnerability testing and management, promptly installing patches, and eliminating or disabling unnecessary services.	CM-3, RA-5
4.8.4.e	Components shall ensure that maintenance ports are disabled during normal system operation and enabled only during approved maintenance activities.	MA-1
4.8.4.f	System libraries shall be managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code.	SI-7
4.8.4.g	Components shall develop maintenance policy and procedures.	MA-1
4.8.4.h	If cleared maintenance personnel are not available, a trusted DHS employee with sufficient technical knowledge to detect and prevent unauthorized modification to the information system or its network shall monitor and escort	MA-5

Policy ID	DHS Policy Statements	Relevant Controls
	the maintenance personnel during maintenance activities. This situation shall only occur in exceptional cases. Components shall take all possible steps to ensure that trusted maintenance personnel are available.	
4.8.4.i	Maintenance using a different user's identity may be performed only when the user is present. The *user* shall log in and observe the maintenance actions at all times. *Users shall not share their authentication information with maintenance personnel.*	MA-5

4.8.5 Personal Use of Government Office Equipment and DHS Systems/Computers

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.a	DHS employees may use Government office equipment and DHS systems/computers for authorized purposes only. "Authorized use" includes limited personal use as described in DHS MD 4600.1, *Personal Use of Government Office Equipment*, and DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*.	---
4.8.5.b	Limited personal use of DHS email and Internet services is authorized for DHS employees as long as this use does not interfere with official duties, inhibit the security of information and information systems, or cause degradation of network services. Specifically prohibited activities include streaming of audio or video, social networking, peer-to-peer networking, software or music sharing/piracy, online gaming, Webmail, Instant Messaging (IM), hacking, and the viewing of pornography or other offensive content. DHS users shall comply with the provisions of DHS MD 4500.1, *DHS Email Usage*, and DHS MD 4400.1, *DHS Web and Information Systems*.	---
4.8.5.c	Anyone granted user account access to any DHS information system (including DHS employees, contractors, and others working on behalf of DHS) shall have no expectations of privacy associated with its use. By completing the authentication process, the user acknowledges his or her consent to monitoring.	AC-8
4.8.5.d	The use of Government office equipment and DHS systems/computers constitutes consent to monitoring and auditing of the equipment/systems at all times. Monitoring includes the tracking of internal transactions and external transactions such as Internet access. It also includes auditing of stored data on local and network storage devices as well as removable media.	AC-8
4.8.5.e	DHS users are required to sign rules of behavior prior to being granted system accounts or access to DHS systems or data. The rules of behavior shall contain a "Consent to Monitor" provision and an acknowledgement that the user has no expectation of privacy.	PL-4

Policy ID	DHS Policy Statements	Relevant Controls
4.8.5.f	Contractors, others working on behalf of DHS, or other non-DHS employees are not authorized to use Government office equipment or information systems/computers for personal use, unless limited personal use is specifically permitted by the contract or memorandum of agreement. When so authorized, the limited personal use policies of this section and the provisions of DHS MD 4600.1, DHS MD 4900, DHS MD 4400.1, and DHS MD 4500.1 shall apply.	---

4.8.6 Wireless Settings for Peripheral Equipment

Peripheral equipment (printers, scanners, fax machines) often includes capabilities, intended to allow wireless access to these devices. Although convenient, wireless access comes with additional risks. In general, wireless access is not allowed on DHS networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.8.6.a	Components shall ensure that wireless capabilities for peripheral equipment are disabled. This applies all to peripherals connected to any DHS network or to systems processing or hosting DHS sensitive data.	CM-7
4.8.6.b	In cases where valid mission requirements or equipment limitations prevent disabling wireless capabilities, Components shall comply with all requirements outlined in Section 4.6, Wireless Communication *and* obtain a waiver or exception in accordance with this policy.	CM-7

4.9 Department Information Security Operations

The DHS Enterprise Operations Center (EOC) is the central coordinating and reporting authority for all Sensitive and National Security computer security incidents throughout the Department. The Homeland Secure Data Network (HSDN) Security Operations Center (SOC) shall report incidents to the DHS EOC through appropriate channels to protect data classification. The HSDN SOC is subordinate to the DHS EOC, acting as the central coordinating and reporting authority for all SECRET computer security incidents throughout the Department.

Policy ID	DHS Policy Statements	Relevant Controls
4.9.a	It is the policy of DHS that employees, contractors, or others working on behalf of DHS have no privacy expectations associated with the use of any DHS network, system, or application. This policy is further extended to anyone who is granted account access to any network, system, or application in use in the Department. By completing the account login process the account owner acknowledges their consent to monitoring.	AC-8, PL-4
4.9.b	Component SOCs and the HSDN SOC shall be operationally subordinate to the DHS EOC, which shall provide them operational oversight and guidance.	IR-1

Policy ID	DHS Policy Statements	Relevant Controls
4.9.c	The DHS EOC or Component SOCs shall lead the coordination and administration of Department and Component policy enforcement points, such as firewalls.	SC-7
4.9.d	The DHS EOC shall implement the Department logging strategy, coordinated with Component SOCs, to enable endpoint visibility and Departmental situational awareness.	—
4.9.e	All SOCs shall have the capability to process intelligence information at the collateral level or above. The DHS EOC and Component SOCs shall have the ability to process SECRET level information continuously and shall have the capability to receive Top Secret / Sensitive Compartmented Information (TS/SCI) information.	IR-4
4.9.f	SOCs shall ensure that personnel are appropriately cleared to access Joint Worldwide Intelligence Communications System (JWICS). SOC managers are free to determine the number and type of personnel to be cleared, but at least one cleared person shall be available per shift. (This person may be on call.) A Government officer shall be available continuously for incident response and management.	IR-4
4.9.g	All Department SOCs shall establish and maintain a forensic capability as outlined in the DHS Enterprise Operations Concept of Operations (EOC CONOPS).	IR-7
4.9.h	Department information security operations shall provide a vulnerability management capability. DHS EOC provides Information Security Vulnerability Management (ISVM) messages and vulnerability assessment capabilities. Component SOCs shall develop a robust vulnerability management capability to compliment the DHS EOC.	SI-5
4.9.i	Component CISOs shall ensure that the DHS CISO is kept apprised of all pertinent matters involving the security of information systems and that security-related decisions and information are distributed to the ISSOs and other appropriate persons.	SI-5
4.9.j	Component SOCs shall report operationally to their respective Component CISO. Each CISO shall exercise oversight over their Component's information security operations functions, including the Component SOCs.	IR-1
4.9.k	The DHS EOC shall report operationally to the DHS CISO.	---

4.10 Security Incidents and Incident Response and Reporting

Policy ID	DHS Policy Statements	Relevant Controls
4.10.a	Components shall establish and maintain a continuous incident response capability.	IR-1
4.10.b	Components shall report *significant incidents* to the DHS EOC by calling (703) 921-6505 as soon as possible but not later than one (1) hour from "validation" (a security event being confirmed as a security incident). Other means of reporting, such as the EOC ONLINE portal (https://eoconline.dhs.gov) are acceptable, but the Component shall positively verify that the notification is received and acknowledged by the DHS EOC.	IR-6
4.10.c	Significant HSDN incidents shall be documented with a preliminary report to the HSDN Government Watch Officer or DHS EOC within one hour. An initial detailed report via secure communications shall be provided to the DHS EOC as soon as possible but not later than one hour from "validation." Subsequent updates and status reports shall be provided to the DHS EOC every twenty-four (24) hours or when new information is discovered via HSDN SOC ONLINE until incident resolution. Significant incidents are reported individually on a per incident basis and shall not be reported in the monthly summary report. Additional guidance is located in DHS 4300A, "Incident Response and Reporting," Attachment F Section 3.0 of the *DHS 4300A Sensitive Systems Handbook*.	IR-6
4.10.d	Components shall report minor incidents in the weekly incident report. SBU systems may report via the DHS EOC portal (https://eoconline.dhs.gov). Components with no portal access shall report minor incidents via email to dhs.soc@dhs.gov. HSDN incidents or incidents involving SECRET information shall be documented in a summary report via the HSDN DHS EOC portal.	IR-6
4.10.e	DHS personnel shall follow DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with the DHS EOC CONOPS. Reports shall be classified at the highest classification level of the information contained in the document. Unsanitized reports shall be marked and handled appropriately.	IR-1
4.10.f	If a DHS Component has no incidents to report for a given week, a weekly "No Incidents" report shall be sent to the EOC.	IR-6
4.10.g	The DHS EOC shall report incidents to the United States Computer Emergency Readiness Team (US-CERT), in accordance with the DHS EOC CONOPS. Components shall not send incident reports directly to US-CERT.	IR-6
4.10.h	The DHS EOC shall receive classified spillage incident reports, and support the DHS CSO for containment and cleanup. All classified spillages are significant incidents.	IR-6

Policy ID	DHS Policy Statements	Relevant Controls
4.10.i	The DHS EOC shall maintain information security "playbooks," checklists that implement procedures and provide guidance on how to respond rapidly to developing incidents.	IR-1
4.10.j	The DHS EOC shall respond to detected faults, attacks, events, or incidents and communicate incident reports to external organizations that may be affected.	IR-1
4.10.k	Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS EOC. The DHS EOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F to the *DHS 4300A Sensitive Systems Handbook*.	IR-7
4.10.l	Components shall develop and publish internal computer security incident response plans and incident handling procedures, and provide copies to the DHS CSIRC. Each procedure shall include a detailed CM process for modification of security device configurations.	IR-1
4.10.m	Component Heads shall take corrective actions when security incidents and violations occur and shall hold personnel accountable for intentional transgressions.	IR-1
4.10.n	The DHS EOC shall monitor and report incident investigation and incident remediation activities to the DHS Chief Information Officer (CIO) and CISO in accordance with the DHS EOC CONOPS until the incident is closed.	IR-5
4.10.o	The DHS CISO shall determine the frequency and content of security incident reports.	IR-6
4.10.p	The Component CSIRC shall report incidents only to the DHS EOC and to no other external agency or organization.	IR-6
4.10.q	The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required.	IR-1
4.10.r	The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO.	IR-3

4.10.1 Law Enforcement Incident Response

The DHS EOC shall notify the DHS Chief, Internal Security and Investigations Division, Office of Security (CISID-OIS) whenever an incident requires law enforcement involvement. Law enforcement shall coordinate with the DHS EOC, the CISID-OIS, the Component, and other appropriate parties whenever a crime is committed or suspected.

Policy ID	DHS Policy Statements	Relevant Controls
4.10.1.a	Components shall coordinate all external law enforcement involvements through the DHS EOC and obtain guidance from the DHS EOC before contacting local law enforcement. Exceptions are only made during emergencies where there is risk to life, limb, or property. In cases of emergency notification, the Component shall notify the DHS EOC as soon as possible, by the most expedient means available.	IR-6
4.10.1.b	Security Incidents may include law enforcement (LE) or counter intelligence (CI) elements, such as maintaining a chain of custody. All incidents containing a LE/CI aspect shall be coordinated with the DHS CSO through the DHS EOC.	IR-6

4.11 Documentation

Policy ID	DHS Policy Statements	Relevant Controls
4.11.a	Components shall ensure that information systems and networks are appropriately documented in such a way as to allow others to understand system operation and configuration.	CM-8
4.11.b	System Owners shall update system documentation annually or whenever significant changes occur. Changes that may require updates include: • New threat information • Weaknesses or deficiencies discovered in currently deployed security controls after an information system breach • A redefinition of mission priorities or business objectives resulting in a change to the security category of the information system • A change in the information system (e.g., adding new hardware, software, or firmware; or establishing new connections) or the system's environment of operation	CM-3, CM-8, SA-5
4.11.c	Documentation shall be kept on hand and shall be accessible to authorized personnel (including auditors) at all times.	CM-3
4.11.d	System documentation may be categorized as Sensitive if deemed appropriate by the Component CISO/ISSM. This category shall not be used as a means of restricting access to auditors or other authorized personnel.	CM-3

4.12 Information and Data Backup

Policy ID	DHS Policy Statements	Relevant Controls
4.12.a	The policies in this document, including Security Authorization Process	---

Policy ID	DHS Policy Statements	Relevant Controls
	requirements, apply to any devices that process or host DHS data.	
4.12.b	Component CISOs/ISSMs shall determine whether or not automated process devices shall be included as part of an information system's Security Authorization Process requirements.	---

4.13 Converging Technologies

Advances in technology have resulted in the availability of devices that offer multiple functions. Many devices such as multifunctional desktop computers, copiers, facsimile machines, and heating, ventilation and air conditioning (HVAC) systems may contain sensitive data and may also be connected to data communications networks.

Policy ID	DHS Policy Statements	Relevant Controls
4.13.a	The policies in this document apply to any networked devices that contain Information Technology (IT), including copiers, facsimile machines, and alarm control systems.	---
4.13.b	Components shall ensure that network printers and facsimile machines are updated to the latest version of their firmware/software at least annually.	CM-2
4.13.c	Components shall ensure that network printers, copiers, and facsimile machines are configured for least required functionality.	CM-7
4.13.d	Components shall ensure that each network printer, copier, and facsimile machine is within the system definition of a DHS information system that has a current ATO.	CM-8
4.13.e	Components shall ensure that remote maintenance of network printers, copiers, and facsimile machines is conducted only from within DHS networks. If maintenance planning does not include performing remote maintenance, Components shall ensure that remote maintenance capabilities are disabled.	MA-4
4.13.f	Components shall ensure that network printers, copiers, and facsimile machines are configured to restrict administrator access to authorized individuals or groups.	MA-5
4.13.g	Components shall ensure that maintenance or disposal of network printers, copiers, or facsimile machines, approved for sensitive reproduction, is performed only while escorted by a properly cleared person with knowledge to detect any inappropriate action.	MA-5
4.13.h	Components shall ensure that memory and hard drives do not leave the facility; they are to be replaced and the old part destroyed as sensitive media.	MP-6

Policy ID	DHS Policy Statements	Relevant Controls
4.13.i	Components shall locate network printers, copiers, and facsimile machines approved to process sensitive information in areas where access can be controlled when paper output is being created.	PE-18
4.13.j	Any multifunction device connected to a DHS network or other information system containing sensitive data shall have the inbound dial in capabilities disabled.	AC-17

5.0 TECHNICAL POLICIES

The design of information systems that process, store, or transmit sensitive information shall include the automated security features discussed in this section. Security safeguards shall be in place to ensure that each person having access to sensitive information systems is individually accountable for his or her actions while utilizing the system.

5.1 Identification and Authentication

Policy ID	DHS Policy Statements	Relevant Controls
5.1.a	Components shall ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.	IA-1, IA-2
5.1.b	For information systems requiring authentication controls, Components shall ensure that the information system is configured to require that each user be authenticated before information system access occurs.	IA-1, IA-2
5.1.c	For systems with low impact for the confidentiality security objective, Components shall disable user identifiers after ninety (90) days of inactivity; for systems with moderate and high impacts for the confidentiality security objective, Components shall disable user identifiers after forty-five (45) days of inactivity.	IA-4
5.1.d	Department of Homeland Security (DHS) users shall not share identification or authentication materials of any kind, nor shall any DHS user allow any other person to operate any DHS system by employing the user's identity.	IA-5
5.1.e	All user authentication materials shall be treated as sensitive material and shall carry a classification as high as the most sensitive data to which that user is granted access using that authenticator.	IA-7
5.1.f	Components shall implement strong authentication on servers, for system administrators and personnel with significant security responsibilities, within six (6) months of the Component's implementation of Homeland Security Presidential Directive (HSPD) HSPD-12.	IA-2
5.1.g	Where available, PIV credentials shall be used as the primary means of logical authentication for DHS sensitive systems.	—

5.1.1 Passwords

The least expensive method for authenticating users is a password system in which authentication is performed each time a password is used. More sophisticated authentication techniques, such as Smart Cards and biological recognition systems (e.g., retina scanner, handprint, voice recognition), shall be cost-justified through the risk assessment process.

Policy ID	DHS Policy Statements	Relevant Controls
5.1.1.a	In those systems where user identity is authenticated by password, the system Information Systems Security Officer (ISSO) shall determine and enforce appropriate measures to ensure that strong passwords are used.	IA-5
5.1.1.b	The ISSO shall determine and enforce the appropriate frequency for changing passwords in accordance with appropriate guidance documentation (if published). In the absence of specific guidance documentation, passwords shall not remain in effect longer than ninety (90) days.	IA-5
5.1.1.c	DHS users shall not share personal passwords.	IA-5
5.1.1.d	Use of group passwords is limited to situations dictated by operational necessity or critical for mission accomplishment. Use of a group User ID and password shall be approved by the appropriate Authorizing Official (AO).	IA-4
5.1.1.e	Components shall prohibit passwords from being embedded in scripts or source code.	IA-5
5.1.1.f	Components shall ensure that all passwords are stored in encrypted form.	IA-5

The use of a personal password by more than one individual is prohibited throughout DHS. It is recognized, however, that, in certain circumstances such as the operation of crisis management or operations centers, watch team and other duty personnel may require the use of group User IDs and passwords.

5.2 Access Control

Policy ID	DHS Policy Statements	Relevant Controls
5.2.a	Components shall implement access control policy and procedures that provide protection from unauthorized alteration, loss, unavailability, or disclosure of information.	AC-1
5.2.b	Access control shall follow the principles of least privilege and separation of duties and shall require users to use unique identifiers. *Social Security Numbers shall not be used as login IDs.*	AC-2, IA-1
5.2.c	Users shall not provide their passwords to anyone, including system administrators.	IA-5
5.2.d	Emergency and temporary access authorization shall be strictly controlled and shall be approved by the Component Chief Information Security Officer (CISO) or Information Systems Security Manager (ISSM) or his/her designee prior to being granted.	AC-2

Policy ID	DHS Policy Statements	Relevant Controls
5.2.e	System Owners shall ensure that users are assigned unique account identifiers.	AC-2, IA-4
5.2.f	DHS systems with a Federal Information Processing Standard (FIPS) 199 confidentiality categorization of high shall limit the number of concurrent sessions for any user to one (1) unless strong authentication is used.	AC-10
5.2.g	Components and Programs shall ensure that all data-at-rest, particularly in cloud or other virtual environments, preserves its identification and access requirements (anyone with access to data storage containing more than one type of information must have specific access authorization for every type of data in the data storage.	---

5.2.1 Automatic Account Lockout

Components shall configure each information system to lock a user's account for a specified period following a specified number of consecutive failed logon attempts. Users shall be locked from their account for a period of twenty (20) minutes after three consecutive failed logon attempts. All failed logon attempts must be recorded in an audit log and periodically reviewed.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.1.a	Components shall configure accounts to automatically lock a user's *account* after three consecutive failed logon attempts.	AC-7
5.2.1.b	The automatic lockout period for accounts locked due to failed login attempts shall be set for twenty (20) minutes.	AC-7
5.2.1.c	Components shall establish a process for manually unlocking accounts prior to the expiration of the twenty (20) minute period, after sufficient user identification is established. This may be accomplished through the help desk.	AC-7

5.2.2 Automatic Session Termination

The term *session* refers to a connection between a terminal device (workstation, laptop, PED) and a networked application or system.. The term does not include a direct connection to a DHS network, as when authenticating from a device that is directly connected to a DHS network.)The term *session* also refers to accessing an application or system such as a database or networked application through the DHS network. When a session is locked, the user may resume activity by reauthenticating.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.2.a	Components shall configure networked applications or systems to automatically lock any user session in accordance with the appropriate configuration guide. In the absence of configuration guidance, the session shall lock following twenty (20) minutes of inactivity.	AC-11
5.2.2.b	Locked sessions shall remain locked until the user re-authenticates.	AC-11
5.2.2.c	Sessions shall automatically be terminated after sixty (60) minutes of inactivity.	SC-10

5.2.3 Warning Banner

The DHS CISO stipulates that a warning banner statement be displayed on all DHS systems during logon. The most current language can be found on the DHS CISO Web page.

Please note that the current warning banner was developed specifically for use on DHS workstations. Due to differing function, purpose and situation as well as length requirements, warning banners for other environments, such as routers, switches and public-facing websites, will be developed and included in a future version of the *DHS 4300A Sensitive Systems Handbook*.

The use of the warning banner serves as a reminder to all users that the computers they are accessing are Government computers.

Policy ID	DHS Policy Statements	Relevant Controls
5.2.3.a	Systems internal to the DHS network shall display a warning banner specified by the DHS CISO.	AC-8
5.2.3.b	Systems accessible to the public shall provide both a security and a privacy statement at every entry point.	AC-8

5.3 Auditing

Policy ID	DHS Policy Statements	Relevant Controls
5.3.a	Audit records shall be sufficient in detail to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit records shall be reviewed as specified in the SP. The audit record shall contain at least the following information: - Identity of each user and device accessing or attempting to access the system - Time and date of the access and the logoff - Activities that might modify, bypass, or negate information security safeguards - Security-relevant actions associated with processing - All activities performed using an administrator's identity	AU-3
5.3.b	Audit records for financial systems or for systems hosting or processing Personally Identifiable Information (PII) shall be reviewed each month. Unusual activity or unexplained access attempts shall be reported to the System Owner and Component CISO/ISSM.	AU-6
5.3.c	Components shall ensure that their audit records and audit logs are protected from unauthorized access, modification, or destruction.	AU-9
5.3.d	Components shall ensure that audit logs are recorded and retained in accordance with the Component's Record Schedule or with the DHS Records Schedule. At a minimum audit trail records shall be maintained online for at least ninety (90) days. Audit trail records shall be preserved for a period of seven (7) years as part of managing records for each system to allow audit information to be placed online for analysis with reasonable ease.	AU-11
5.3.e	Components shall evaluate the system risks associated with extracts of PII from databases. If the risk is determined to be sufficiently high, a procedure shall be developed for logging computer-readable data extracts. If logging these extracts is not possible, this determination shall be documented, and compensating controls identified in the SP.	AU-1, AU-2, AU-3, PM-9
5.3.f	Component Security Operations Centers (SOC) shall implement both general and threat-specific logging.	AU-1

5.4 Network and Communications Security

5.4.1 Remote Access and Dial-In

Remote access technology allows trusted employees to access DHS networks by dialing in via modem or accessing the DHS network via the Internet. This allows mobile employees to stay in touch with the home office while traveling. There are significant security risks, however,

associated with remote access and dial-in capabilities. Proper procedures can help mitigate these risks.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.1.a	Data communication connections via modem shall be limited and shall be tightly controlled, as such connections can be used to circumvent security controls intended to protect DHS networks. Data communication connections are not allowed unless they have been authorized by the Component CISO/ISSM. Approved remote access to DHS networks shall only be accomplished through equipment specifically approved for that purpose. Tethering with wireless PEDs is prohibited unless approved by the appropriate AO.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.b	Components shall centrally manage all remote access and dial-in connections to their systems and shall ensure that remote access and approved dial-in capabilities provide strong two-factor authentication, audit capabilities, and protection for sensitive information throughout transmission. DHS has an immediate goal that remote access shall only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. Any two-factor authentication shall be based on Department-controlled certificates or hardware tokens issued directly to each authorized user. Remote access solutions shall comply with the encryption requirements of FIPS 140-2, *Security Requirements for Cryptographic Modules*. See Section 3.14 of this Policy Directive, "Privacy and Data Security" for additional requirements involving remote access of PII.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.c	Remote access of PII shall comply with all DHS requirements for sensitive systems, including strong authentication. Strong authentication shall be accomplished by means of virtual private network (VPN) or equivalent encryption and two-factor authentication. The Risk Assessment and Security Plan (SP) shall document any remote access of PII, and the remote access shall be approved by the AO prior to implementation.	AC-4, AC-17, AU-2 SC-7, SC-8, SC-9
5.4.1.d	Remote access of PII shall not permit the download and remote storage of information unless the requirements for the use of removable media with sensitive information have been addressed. All downloads shall follow the concept of least privilege and shall be documented with the SP.	---

5.4.2 Network Security Monitoring

Security monitoring, detection, and analysis are key functions and are critical to maintaining the security of DHS information systems. Network monitoring and analysis is limited to observing network activity for anomalies, malicious activities and threat profiles. Content analysis is not within the scope of network monitoring.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.2.a	Components shall provide continuous monitoring of their networks for security events, or outsource this requirement to the DHS Enterprise Operations Center (EOC). Monitoring includes interception and disclosure as to the extent necessary for rendering service or to protect Department or Component rights or property. Here *rights* refers to ownership or entitlements or to property or information as in intellectual property. Service observation or random monitoring shall not be used except for mechanical or service quality control checks in accordance with the Electronic Communications Privacy Act	SI-4
5.4.2.b	The DHS EOC shall administer and monitor DHS intrusion detection system (IDS) sensors and security devices.	SI-4
5.4.2.c	Component SOCs shall administer and monitor Component IDS sensors and security devices.	SI-4

5.4.3 Network Connectivity

A system interconnection is the direct connection of two or more information systems for the purpose of sharing data and other information resources by passing data between each other via a direct system-to-system interface without human intervention. Any physical connection that allows other systems to share data (pass thru) also constitutes an interconnection, even if the two systems connected do not share data between them. System interconnections do not include instances of a user logging on to add or retrieve data, nor users accessing Web-enabled applications through a browser.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.3.a	Components shall ensure that appropriate identification and authentication controls, audit logging, and access controls are implemented on every network element.	AC-1, AC-2, AU-1, AU-2, IA-1, IA-2
5.4.3.b	Interconnections between DHS and non-DHS systems shall be established only through controlled interfaces and by approved service providers. The controlled interfaces shall be authorized at the highest security level of information on the network. Connections with other Federal agencies shall be documented based on interagency agreements, memorandums of understanding, service level agreements or interconnection security agreements.	CA-3
5.4.3.c	Components shall document all interconnections to the DHS OneNet with an ISA signed by the OneNet AO and by each appropriate AO. Additional information on ISAs is published in, "Preparation of Interconnection Security	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
	Agreements," Attachment N to the *DHS 4300A Sensitive Systems Handbook*.	
5.4.3.d	ISAs shall be reissued every three (3) years or whenever any significant changes have been made to any of the interconnected systems.	CA-3
5.4.3.e	ISAs shall be reviewed and updated as needed as a part of the annual Federal Information Security Management Act (FISMA) self-assessment.	CA-3
5.4.3.f	Components may complete a master Interconnection Security Agreement (ISA) that includes all transitioning systems as part of their initial OneNet transition. After transition, each additional system or General Support System (GSS) shall be required to have a separate ISA. Interconnections between DHS Components (not including DHS OneNet) shall require an ISA whenever there is a difference in the security categorizations for confidentiality, integrity, and availability between the systems or when the systems do not share the same security policies. (In this context, *security policies* refers to the set of rules that controls a system's working environment, and not to DHS information security policy). ISAs shall be signed by the appropriate AO.	---
5.4.3.g	Components shall document interconnections between their own and external (non-DHS) networks with an ISA for each connection.	CA-3
5.4.3.h	The DHS Chief Information Officer (CIO) shall approve all interconnections between DHS enterprise-level information systems and non-DHS information systems. The DHS CIO shall ensure that connections with other Federal Government agencies are properly documented. A single ISA may be used for multiple connections provided that the security authorization is the same for all connections covered by that ISA.	CA-3
5.4.3.i	The Department and Components shall implement Trust Zones by means of Policy Enforcement Points (PEP), as defined in the DHS Security Architecture.	SC-7
5.4.3.j	DHS OneNet shall provide secure Name/Address resolution service. Domain Name System Security Extensions (DNSSEC) has been designated as the DHS service solution.	SC-20, SC-21, SC-22
5.4.3.k	All DHS systems connected to OneNet and operating at moderate or high level shall utilize secure Name/Address resolution service provided by DHS OneNet.	SC-20, SC-21, SC-22
5.4.3.l	The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB.	CM-3
5.4.3.m	Interconnections between two authorized DHS systems do not require an ISA	CA-3

Policy ID	DHS Policy Statements	Relevant Controls
	if the interface characteristics, security requirements, nature of information communicated and monitoring procedures for verifying enforcement of security requirements are accounted for in the SPs or are described in another formal document, such as a Service Level Agreement (SLA) or contract, and the risks have been assessed and accepted by all involved AOs.	
5.4.3.n	Granting the ability to log into one DHS system through another DHS system (such as through OneNet trust) does not require an ISA, when the requirements from Section 5.4.3.m are met.	---

5.4.4 Firewalls and Policy Enforcement Points

Policy Enforcement Points (PEP) separate Trust Zones as defined in the DHS Security Architecture. Boundary protection between DHS and external networks is implemented by firewalls at the TICs and other approved direct system inter-connections. DHS TICs are provided by OneNet and monitored by the DHS EOC. Component SOCs may protect DHS-internal boundaries across Trust Zones.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.a	Components shall restrict physical access to firewalls and PEP to authorized personnel.	AC-4, SC-7
5.4.4.b	Components shall implement identification and strong authentication for administration of the firewalls and PEPs.	AC-4, SC-7
5.4.4.c	Components shall encrypt remote maintenance paths to firewalls and PEPs.	MA-4, SC-7
5.4.4.d	Components shall conduct quarterly firewall and PEP testing to ensure that the most recent policy changes have been implemented and that *all* applied policies and controls are operating as intended.	SC-7
5.4.4.e	Component SOCs shall ensure that reports on information security operations status and incident reporting are provided to the DHS CISO as required.	IR-6
5.4.4.f	All Department and Component firewalls and PEPs shall be administered in coordination with DHS security operation capabilities, through the DHS EOC/SOC or Component SOC.	SC-7
5.4.4.g	All DHS PEPs shall provide protection against denial-of-service attacks.	SC-5
5.4.4.h	Components shall determine protocols and services permitted through their Component-level PEPs. Components may restrict traffic sources and destinations at their Component-level PEPs.	SC-7

Policy ID	DHS Policy Statements	Relevant Controls
5.4.4.i	The DHS CISO shall establish policy to block or allow traffic from sources and to destinations at the DHS TIC PEPs. The DHS CISO policy shall prevent traffic as directed by the DHS CIO.	SC-7
5.4.4.j	The DHS EOC shall oversee all enterprise PEPs.	---

5.4.5 Internet Security

Policy ID	DHS Policy Statements	Relevant Controls
5.4.5.a	Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS TIC PEPs. The PSTN shall not be connected to OneNet at any time.	SC-7
5.4.5.b	Firewalls and PEPs shall be configured to prohibit any protocol or service that is not explicitly permitted.	CM-7, SC-7, SC-8, SC-9
5.4.5.c	Components shall ensure that all executable code, including mobile code (e.g., ActiveX, JavaScript), is reviewed and approved by the Program Manager prior to the code being allowed to execute within the DHS environment. [Note: When the technology becomes available and code can be vetted for security, the policy will be "Ensure that all approved code, including mobile code (e.g., ActiveX, JavaScript), is digitally signed by the designated DHS authority and that only signed code is allowed to execute on DHS systems."]	SC-18
5.4.5.d	Telnet shall not be used to connect to any DHS computer. A connection protocol such as Secure Shell (SSH) that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.e	File Transfer Protocol (FTP) shall not be used to connect to or from any DHS computer. A connection protocol that employs secure authentication (two factor, encrypted, key exchange) and is approved by the Component shall be used instead.	CM-7, SC-7, SC-8, SC-9
5.4.5.f	Remote Desktop connections, such as Microsoft's Remote Desktop Protocol (RDP), shall not be used to connect to or from any DHS computer without the use of an authentication method that employs secure authentication (two-factor, encrypted, key exchange).	AC-17, IA-2
5.4.5.g	In order to ensure the security and availability of DHS information and information systems, the DHS CIO or DHS CISO may direct that specific Internet websites or categories be blocked at the DHS TICs, on advice from the United States Computer Emergency Readiness Team (US-CERT), the	---

Policy ID	DHS Policy Statements	Relevant Controls
	DHS EOC, or other reputable sources.	

5.4.6 Email Security

The DHS email gateway Steward provides email monitoring for spam and virus activity at the gateway.

DHS EOC personnel shall be trained to respond to incidents pertaining to email security and shall assist the email gateway Steward as necessary. Components shall provide appropriate security for their email systems.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.6.a	Components shall correctly secure, install, and configure the underlying email operating system.	---
5.4.6.b	Components shall correctly secure, install, and configure mail server software.	---
5.4.6.c	Components shall secure and filter email content.	---
5.4.6.d	Components shall deploy appropriate network protection mechanisms, such as: - Firewalls - Routers - Switches - Intrusion detection systems	---
5.4.6.e	Components shall secure mail clients.	---
5.4.6.f	Components shall conduct mail server administration in a secure manner. This includes: - Performing regular backups - Performing periodic security testing - Updating and patching software - Reviewing audit logs at least weekly	---
5.4.6.g	The DHS email gateway Steward shall provide email monitoring for malware activity at the gateway.	SI-3
5.4.6.h	The DHS email gateway Steward shall provide email monitoring for spam at the gateway.	SI-8
5.4.6.i	Auto-forwarding or redirecting of DHS email to any address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually	---

Policy ID	DHS Policy Statements	Relevant Controls
	forward individual messages after determining that the risks or consequences are minimal.	
5.4.6.j	All DHS email systems are required to use the common naming convention with distinguishing identifiers for military officers, contractors, foreign nationals, and U.S. Government personnel from other Departments and agencies.	---

Note: Due to the significant risk associated with HTML email, DHS is considering following the lead of the Department of Defense (DoD) and moving to text based email.

5.4.7 Personal Email Accounts

Policy ID	DHS Policy Statements	Relevant Controls
5.4.7.a	The use of Internet Webmail (Gmail, Yahoo, AOL) or other personal email accounts is not authorized over DHS furnished equipment or network connections.	---
5.4.7.b	When sending email containing any sensitive information, particularly sensitive PII, users should use caution. When sending such information outside the dhs.gov domain, users shall ensure the information is attached as an encrypted file.	---

5.4.8 Testing and Vulnerability Management

The DHS EOC takes a proactive approach to vulnerability management including detecting vulnerabilities through testing, reporting through Information System Vulnerability Management (ISVM) messages, and conducting Vulnerability Assessments (VA).

Vulnerability management is a combination of detection, assessment, and mitigation of weaknesses within a system. Vulnerabilities may be identified from a number of sources, including reviews of previous risk assessments, audit reports, vulnerability lists, security advisories, and system security testing such as automated vulnerability scanning or security control assessments.

Core elements of vulnerability management include continuous monitoring and mitigating the discovered vulnerabilities, based on a risk management strategy. This strategy accounts for vulnerability severity, threats, and assets at risk.

Policy ID	DHS Policy Statements	Relevant Controls
5.4.8.a	Components shall conduct vulnerability assessments and/or testing to identify security vulnerabilities on information systems containing sensitive information annually or whenever significant changes are made to the information systems. This shall include scanning for unauthorized wireless	---

Policy ID	DHS Policy Statements	Relevant Controls
	devices on the network. Evidence that annual assessments have been conducted shall be included in SARs and with annual security control assessments.	
5.4.8.b	Component CISOs/ISSMs shall approve and manage all activities relating to requests for Vulnerability Assessment Team (VAT) assistance in support of incidents, internal and external assessments, and on-going SLC support.	---
5.4.8.c	Component CISOs/ISSMs or their designated representatives shall acknowledge receipt of ISVM messages.	SI-5
5.4.8.d	Components shall report compliance with the ISVM message within the specified time. Components not able to do so shall submit documentation of a waiver request via the DHS EOC Online Portal (https://eocotline.dhs.gov).	SI-5
5.4.8.e	When vulnerability assessment responsibilities encompass more than one Component, Component CISOs/ISSMs shall coordinate with the relevant Component SOC and the DHS EOC.	RA-3
5.4.8.f	The DHS EOC shall be notified before any ISVM scans are run.	RA-5
5.4.8.g	System Owners shall report the security alert and advisory status of the information system to the AO, Component CISO/ISSM, and DHS CISO upon request and on a periodic basis.	SI-5

5.4.9 Peer-to-Peer Technology

Policy ID	DHS Policy Statements	Relevant Controls
5.4.9.a	Peer to peer software technology is prohibited on any DHS information system.	CM-7, SA-6

5.5 Cryptography

Cryptography is a branch of mathematics that deals with the transformation of data. Cryptographic transformation converts ordinary text (plaintext) into coded form (ciphertext) by encryption; and ciphertext into plaintext by decryption.

5.5.1 Encryption

Encryption is the process of changing plaintext into ciphertext for the purpose of security or privacy.

Policy ID	DHS Policy Statements	Relevant Controls
5.5.1.a	Systems requiring encryption shall comply with the following methods:	IA-7,

Policy ID	DHS Policy Statements	Relevant Controls
	• Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that have been validated under FIPS 140-2 • National Security Agency(NSA) Type 2 or Type 1 encryption (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)	SC-13
5.5.1.b	Components shall develop and maintain encryption plans for sensitive information systems.	IA-7, SC-13
5.5.1.c	Components shall use only cryptographic modules that are FIPS 197 (AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.	IA-7, SC-13

5.5.2 Public Key Infrastructure

A PKI is an architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures.

The principal components of a PKI are the public key certificates, registration authorities (RA), certification authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy (CP.)

Policy ID	DHS Policy Statements	Relevant Controls
5.5.2.a	The DHS CISO shall be the DHS PKI Policy Authority (PKI PA) to provide PKI policy oversight. A detailed description of DHS PKI PA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.b	The DHS CISO shall represent DHS on the Federal PKI Policy Authority (FPKI PA.)	SC-17
5.5.2.c	The DHS PKI PA shall appoint a PKI Management Authority (PKI MA) to provide management and operational oversight of the DHS PKI. A detailed description of DHS PKI MA roles and responsibilities are provided in the DHS PKI Policy.	SC-17
5.5.2.d	The DHS PKI shall be governed by the U.S. Common Policy Framework certificate policy approved by the FPKI PA, and the DHS PKI Policy approved by the DHS PKI PA.	SC-17
5.5.2.e	DHS shall have a single DHS Principal CA that is subordinate to the U.S. Common Policy Root CA (the entity that signs and issues DHS public key certificates). The Principal DHS CA shall be operated for DHS by the	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	Department of Treasury (DoT) under the Federal Shared Service Provider (SSP) program.	
5.5.2.f	All additional CAs within DHS must be subordinate to the DHS Principal CA. The requirements and process for becoming a subordinate CA to the DHS Principal CA shall be specified in the DHS PKI Policy.	SC-17
5.5.2.g	Components that implement a CA shall ensure that the CA is subordinate to the DHS Principal CA.	SC-13
5.5.2.h	All DHS CAs shall have a trust path resolving to the U.S. Common Policy Root CA. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels.	SC-17
5.5.2.i	The DHS Principal CA shall operate under an X.509 Certification Practices Statement (CPS). The CPS shall comply with the U.S. Common Policy Framework. DoT, as the SSP for DHS, approves the CPS for the DHS Principal CA.	SC-17
5.5.2.j	All DHS CAs subordinate to the DHS Principal CA shall operate under an X.509 CPS. The CPS shall comply with the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA must approve the CPS.	SC-17
5.5.2.k	The DHS PKI PA shall ensure that the CPS for each subordinate DHS CA is compliant with the U.S. Common Policy Framework and DHS PKI Policy prior to approval.	SC-17
5.5.2.l	The DHS PKI MA shall ensure that every subordinate DHS CA operates in compliance with its approved CPS.	SC-17
5.5.2.m	All DHS CAs shall undergo regular PKI compliance audits as required by the U.S. Common Policy Framework and the DHS PKI Policy. The DHS PKI PA shall approve the auditor. The audit findings, report, and Plans of Action and Milestones (POA&M) to address deficiencies found shall be provided to the DHS PKI PA and DHS PKI MA.	SC-17
5.5.2.n	All DHS CAs shall archive records as required by the U.S. Common Policy Framework and their CPS.	SC-17
5.5.2.o	All operational PKI facilities shall be established in accordance with U.S. Common Policy Framework physical security requirements based on the CA's assurance level and its intended use. Location/protection of the CA shall be determined by its level of assurance. Measures taken to ensure the continuity of PKI operations shall provide at least the same level of PKI Services availability as the individual and composite availability requirements of the	SC-17

Policy ID	DHS Policy Statements	Relevant Controls
	systems and data protected by the certificates.	
5.5.2.p	The DHS Principal CA and DHS subordinate CAs shall issue certificates only to internal DHS entities, e.g., employees, contractors, roles, groups, applications, code signers, and devices. External entities that require certificates to securely interact with DHS shall acquire certificates from a non-DHS PKI that is cross-certified with the FBCA at medium assurance or above.	SC-17
5.5.2.q	Only the DHS Principal CA shall issue certificates to DHS employees, contractors, roles, code signers, and other human entities, including certificates for DHS HSPD-12 Personal Identity Verification (PIV) Cards. The DHS Principal CA may also issue all other types of certificates allowed under the U.S. Common Policy to internal DHS entities.	SC-17
5.5.2.r	DHS Subordinate CAs shall issue certificates only to internal non-human entities. Any additional restrictions on the types of certificates that may be issued by a specific subordinate DHS CA shall be determined during the subordination process and approved by the DHS PKI PA.	SC-17
5.5.2.s	The use by DHS of any non-DHS service provider for CA or PKI services is prohibited unless approved by the DHS CISO.	SC-13
5.5.2.t	Only certificates that are issued by the DHS Principal CA or a subordinate DHS CA under the U.S. Common Policy Framework at medium assurance or above shall be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by DHS CAs that are not established as subordinate to the DHS Principal CA, certificates issued by test, pilot, third party, self-signed or other CAs shall not be used to protect sensitive data, or to authenticate to DHS operational systems containing sensitive data.	SC-17

5.5.3 Public Key/Private Key

A public key certificate is used to obtain subscribers' public keys in a trusted manner. Once a certificate is obtained, the public key can be used:

- To encrypt data for that subscriber so that only that subscriber can decrypt it
- To verify that digitally signed data was signed by that subscriber, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.a	Separate public/private key pairs must be used for encryption and digital signature by human subscribers, organization subscribers, application subscribers, and code-signing subscribers.	SC-12

Policy ID	DHS Policy Statements	Relevant Controls
5.5.3.b	Separate public/private key pairs must be used for encryption and digital signature by device subscribers whenever supported by the protocols native to the type of device.	SC-12
5.5.3.c	A human sponsor shall represent each application, role, code-signing, and device subscriber when the subscriber applies for one or more certificates from a DHS CA.	SC-12
5.5.3.d	A DHS sponsor shall be required for DHS contractors or other affiliates who apply for one or more certificates from a DHS CA.	SC-12
5.5.3.e	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine the eligibility of each proposed human, role, application, code signer, or device to receive one or more certificates.	SC-12
5.5.3.f	A mechanism shall be provided for each DHS CA to enable PKI registrars to determine and verify the identity of the authorized human sponsor for each DHS contractor, affiliate, role, application, code signer, or device.	SC-12
5.5.3.g	Human subscribers shall not share private keys and shall be responsible for their security and use. If a human subscriber discloses or shares his or her private key, the subscriber shall be accountable for all transactions signed with the subscriber's private key.	---
5.5.3.h	Sponsors for non-human subscribers (role, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Device Sponsor Agreement" as a pre-condition for sponsoring non-human subscribers.	SC-17
5.5.3.i	Subscriber private keys shall not be used by more than one entity, with the following exception: Multiple devices in a high availability configuration may use a single Secure Socket Layer (SSL) Subject Alternative Name (SAN) certificate, and thus use the same key pair.	SC-12
5.5.3.j	Every human subscriber shall read, understand, and sign a "DHS PKI Human Subscriber Agreement" as a pre-condition for receiving certificates from a DHS CA. Signed PKI Human Subscriber Agreements shall be maintained by the DHS PKI MA.	SC-17

5.6 Malware Protection

Policy ID	DHS Policy Statements	Relevant Controls
5.6.a	Component CISOs/ISSMs shall establish and enforce Component-level	SI-3

Policy ID	DHS Policy Statements	Relevant Controls
	malware protection control policies.	
5.6.b	Components shall implement a defense-in-depth strategy that: - Installs antivirus software on desktops and servers - Configures antivirus software on desktops and servers to check all files, downloads, and email - Installs updates to antivirus software and signature files on desktops and servers in a timely and expeditious manner without requiring the end user to specifically request the update - Installs security patches to desktops and servers in a timely and expeditious manner	SI-3
5.6.c	System Owners shall develop and enforce procedures to ensure proper malware scanning of media prior to installation of primary hard drives, software with associated files, and other purchased products.	AC-20, SI-3

5.7 Product Assurance

Policy ID	DHS Policy Statements	Relevant Controls
5.7.a	Information Assurance (IA) shall be considered a requirement for all systems used to input, process, store, display, or transmit sensitive or national security information. IA shall be achieved through the acquisition and appropriate implementation of evaluated or validated Commercial off the Shelf (COTS) IA and IA-enabled Information Technology (IT) products. These products shall provide for the availability of systems. The products also shall ensure the integrity and confidentiality of information and the authentication and nonrepudiation of parties in electronic transactions.	---
5.7.b	*Strong preference* shall be given to the acquisition of COTS IA and IA-enabled IT products (to be used on systems entering, processing, storing, displaying, or transmitting sensitive information) that have been evaluated and validated, as appropriate, in accordance with the following: - The National Institute of Standards and Technology (NIST) FIPS validation program - The NSA/NIST National Information Assurance Partnership (NIAP) Evaluation and Validation Program - The International Common Criteria for Information Security Technology Evaluation Mutual Recognition Agreement	---
5.7.c	The evaluation and validation of COTS IA and IA-enabled products shall be	---

Policy ID	DHS Policy Statements	Relevant Controls
	conducted by authorized commercial laboratories or by NIST.	
5.7.d	Components shall use only cryptographic modules that meet the requirements set forth in Section 5.5, Cryptography.	---
5.7.e	Transaction-based systems (e.g., database management systems and transaction processing systems) shall implement transaction rollback and transaction journaling, or technical equivalents.	---

6.0 DOCUMENT CHANGE REQUESTS

Changes to *DHS Sensitive Systems Policy Directive 4300A* and to the DHS 4300A *Sensitive Systems Handbook* may be requested in accordance with Section 1.7, Changes to Policy.

7.0 QUESTIONS AND COMMENTS

For clarification of DHS information security policies or procedures, contact the DHS Director for Information Systems Security Policy at INFOSEC@dhs.gov.

APPENDIX A ACRONYMS AND ABBREVIATIONS

3-DES	Triple Data Encryption Standard
AES	Advanced Encryption Standards
AIS	Automated Information System
A-Number	Alien Registration Number
AO	Authorizing Official
ARB	Acquisition Review Board
ATO	Authority to Operate
BI	Background Investigation
BIA	Business Impact Assessment
BLSR	Baseline Security Requirements
CA	Certification Authority
CBP	Customs and Border Protection
CCB	Change Control Board
CFO	Chief Financial Officer
CI	Counter-Intelligence
CIO	Chief Information Officer
CISID	Chief, Internal Security and Investigations Division
CISID-OIS	Chief, Internal Security and Investigations Division, Office of Security
CISO	Chief Information Security Officer
CM	Configuration Management
CMG	Core Management Group
CMP	Configuration Management Plan
CONOPS	Concept of Operations
COOP	Continuity of Operations Plan Continuity of Operations Planning
COTS	Commercial off the Shelf
CP	Contingency Plan Contingency Planning Certificate Policy

CPIC	Capital Planning and Investment Control
CPS	Certificate Practices Statement
CRE	Computer-Readable Extract
CRL	Certificate Revocation List
CSIRC	Computer Security Incident Response Center
CSO	Chief Security Officer
CUI	Controlled Unclassified Information
DES	Digital Encryption Standards
DHS	Department of Homeland Security
DNSSEC	Domain Name System Security Extensions
DoD	Department of Defense
DoT	Department of Treasury
EA	Enterprise Architecture
EAB	Enterprise Architecture Board
EO	Executive Order
EOC	Enterprise Operations Center
EOC CONOPS	Enterprise Operations Concept of Operations
FAM	Foreign Affairs Manual
FBCA	Federal Bridge Certification Authority
FDCC	Federal Desktop Core Configuration
FEMA	Federal Emergency Management Agency
FICAM	Federal Identity, Credentialing, and Access Management
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management Act
FLETC	Federal Law Enforcement Training Center
FOIA	Freedom of Information Act
FOUO	For Official Use Only
FPKI PA	Federal PKI Policy Authority
FTP	File Transfer Protocol
FYHSP	Future Years Homeland Security Program

GSA	General Services Administration
GSS	General Support System
HIPAA	Health Insurance Portability and Accountability Act
HSAR	Homeland Security Acquisition Regulations
HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HVAC	Heating, Ventilation and Air Conditioning
I&A	Intelligence and Analysis
IA	Identification and Authentication Information Assurance
IATO	Interim Authority to Operate
ICAM	Identity, Credentialing, and Access Management
ICE	Immigration and Customs Enforcement
IDS	Intrusion Detection System
IOC	Initial Operating Capability
IR	Incident Response Infrared
IRB	Investment Review Board
ISA	Interconnection Security Agreement
ISO	Information Security Office
ISSM	Information Systems Security Manager
ISSO	Information Systems Security Officer
ISVM	Information System Vulnerability Management
IT	Information Technology
JWICS	Joint Worldwide Intelligence Communications System
LAN	Local Area Network
LE	Law Enforcement
LMR	Land Mobile Radio
MA	Major Application
MBI	Minimum Background Investigation
MD	Management Directive

MMS	Multimedia Messaging Service
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPPD	National Protection and Programs Directorate
NSA	National Security Agency
OCIO	Office of the Chief Information Officer
OID	Object identifier
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPA	Office of Public Affairs
OPM	Office of Personnel Management
OTAR	Over-The-Air-Rekeying
PA	Policy Authority
PBX	Private Branch Exchange
PCS	Personal Communications Services
PDA	Personal Digital Assistant
PED	Portable Electronic Device
PEP	Policy Enforcement Point
PHI	Protected Health Information
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identity Number
PIRT	Privacy Incident Response Team
PIV	Personal Identity Verification 1.6, 5.5
PKI	Public Key Infrastructure
PKI PA	PKI Policy Authority
PKI MA	PKI Management Authority
PM	Program Manager

PNS	Protected Network Services
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPOC	Privacy Point of Contact
PSTN	Public Switched Telephone Network
PTA	Privacy Threshold Analysis
RDP	Remote Desktop Protocol
RF	Radio Frequency
RFID	Radio Frequency Identification
RMS	Risk Management System
SA	Security Architecture
SAISO	Senior Agency Information Security Officer
SAN	Subject Alternative Name
SAOP	Senior Agency Official for Privacy
SAR	Security Assessment Report
SCAP	Security Content Automation Protocol
SCI	Sensitive Compartmented Information
SELC	Systems Engineering Life Cycle
SLA	Service Level Agreement
SMS	Short Message Service
SOC	Security Operations Center
SORN	System of Records Notice
SP	Special Publication Security Plan
SSH	Secure Shell
SSL	Secure Socket Layer
SSP	Shared Service Provider
Stat.	Statute (refers to a law found in *U.S. Statutes at Large*)
TAF	Trusted Agent FISMA
TFPAP	Trust Framework Provider Adoption Process
TIC	Trusted Internet Connections

TOS	Terms of Service
TRM	Technical Reference Model
TS	Top Secret
TS/SCI	Top Secret, Sensitive Compartmented Information
TSA	Transportation Security Administration
U.S.C.	United States Code
US-CERT	United States Computer Emergency Readiness Team
USCG	United States Coast Guard
USCIS	United States Citizenship and Immigration Service
USGCB	U.S. Government Configuration Baseline
USSS	United States Secret Service
VA	Vulnerability Assessment
VAT	Vulnerability Assessment Team
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
WLAN	Wireless Local Area Network
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

APPENDIX B GLOSSARY

The following definitions apply to the policies and procedures outlined in this document. Other definitions may be found in National Institute of Standards and Technology (NIST) IR 7298, *Glossary of Key Information Security Terms* and the *National Information Assurance (IA) Glossary*.

Acceptable Risk	Mission, organizational, or program-level risk deemed tolerable by the Risk Executive after adequate security has been provided.
Adequate Security	Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. [OMB Circular A-130, Appendix III]
Annual Assessment	Department of Homeland Security (DHS) activity for meeting the annual Federal Information Security Management Act (FISMA) self-assessment requirement.
Authorization Package	The documents submitted to the AO for the Authorization Decision. An Authorization Package consists of: Authorization Decision Letter Security Plan - criteria provided on when the plan should be updated Security Assessment Report - updated on an ongoing basis whenever changes are made to either the security controls in the information system or the common controls inherited by those systems Plan of Action and Milestones (POA&M)
Authorizing Official (AO)	An official within a Federal Government agency empowered to grant approval for a system to operate.
Certification/ Certifying Agent	A contractor that performs certification tasks as designated by the CO.
Certificate (or Certifying) Authority (CA)	A trusted third party that issues certificates and verifies the identity of the holder of the digital certificate.
Chief Information Officer (CIO)	The executive within a Federal Government agency responsible for its information systems.
Compensating Control	An internal control intended to reduce the risk of an existing or potential control weakness.

Component	A DHS Component is any of the entities within DHS, including every DHS office and independent agencies.
Computer Security Incident Response Center	DHS organization that responds to computer security incidents.
Designated Approval Authority (DAA)	Obsolete term; see Authorizing Official (AO).
Enterprise Operations Center (EOC)	The DHS organization that coordinates security operations for the DHS Enterprise.
Exception	Acceptance to permanently operate a system that does not comply with policy.
For Official Use Only (FOUO)	The marking instruction or caveat "For Official Use Only" will be used within the DHS community to identify sensitive but unclassifed information that is not otherwise specifically described and governed by statute or regulation.
General Support System (GSS)	An interconnected set of information resources under the same direct management control and sharing common functionality. A GSS normally includes hardware, software, information, applications, communications, data, and users.
Information Security Vulnerability Management (ISVM)	A DHS system that provides notification of newly discovered vulnerabilities, and tracks the status of vulnerability resolution.
Information System	Any information technology that is (1) owned, leased, or operated by any DHS Component, (2) operated by a contractor on behalf of DHS, or (3) operated by another Federal, state, or local Government agency on behalf of DHS. Information systems include general support systems and major applications (MA).
Information System Security Officer (ISSO)	A Government employee or contractor who implements and/or monitors security for a particular system.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

Major Application (MA)	An automated information system (AIS) that "requires special attention to security due to the risk and magnitude of harm that can result from the loss, misuse, or unauthorized access to or modification of the information in the application" in accordance with OMB Circular A-130. An MA is a discrete application, whereas a GSS may support multiple applications.
Management Controls	The security controls for an information system that focus on the management of risk and the management of information system security.
Operational Controls	The security controls for an information system that are primarily implemented and executed by people (as opposed to being executed by systems).
Operational Risk	The risk contained in a system under operational status. It is the risk that an AO accepts when granting an ATO.
Personally Identifiable Information (PII)	Any information that permits the identity of an individual to be directly or indirectly inferred, including any other information that is linked or linkable to an individual regardless of whether the individual is a U.S. Citizen, legal permanent resident, or a visitor to the U.S.
Pilot	A test system in the production environment that may contain operational data and may be used to support DHS operations, typically in a limited way.
Policy Enforcement Point (PEP)	A firewall or similar device that can be used to restrict information flow.
Policy Statement	A high-level rule for guiding actions intended to achieve security objectives.
Portable Electronic Device (PED)	A device that has a battery and is meant to process information without being plugged into an electric socket; it is often handheld but can be a laptop computer.
Privacy Sensitive System	Any system that collects, uses, disseminates, or maintains *PII* or sensitive PII.
Production	The applications and systems that DHS end users access and use operationally to execute business transactions.
Prototype	A test system in a test environment that must not contain operational data and must not be used to support DHS operations.

Remote Access	Access to a DHS information system by a user (or an information system) communicating through an external, non-DHS-controlled network (e.g., the Internet).
Residual Risk	The risk remaining after security controls have been applied.
Risk Executive (RE)	An individual who ensures that risks are managed consistently across the organization. An RE can be at the Departmental or Component level.
Security Control	A particular safeguard or countermeasure to protect the confidentiality, integrity, and availability of a system and its information.
Security Control Assessor	A senior management official who certifies the results of the security control assessment. He or she must be a Federal Government employee.
Security Incident	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits, or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Security Operations Center (SOC)	The organization in each DHS Component that coordinates the Component's security operations.
Security Requirement	A formal statement of action or process applied to an information system and its environment in order to provide protection and attain security objectives. Security requirements for any given system are contained in its Security Plan.
Senior Agency Information Security Official (SAISO)	The point of contact within a Federal Government agency responsible for its information system security.
Sensitive But Unclassified	Obsolete designation; see Sensitive Information.
Sensitive Information	Information not otherwise categorized by statute or regulation that if disclosed could have an adverse impact on the welfare or privacy of individuals or on the welfare or conduct of Federal Government programs or other programs or operations essential to the national interest.
Sensitive Personally Identifiable Information (Sensitive PII)	PII that requires stricter handling guidelines because of the nature of the data and the increased risk to an individual if compromised, and if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples of sensitive PII include Social Security numbers and Alien Registration Numbers (A-number).
Significant Incident	A computer security-related incident that represents a meaningful threat to the DHS mission and requires immediate leadership notification.

Spam	Emails containing unwanted commercial solicitation, fraudulent schemes, and possibly malicious logic.
Strong Authentication	Layered authentication approach relying on two or more authenticators to establish the identity of an originator or receiver of information.
System	A discrete set of information system assets contained within the authorization boundary.
System Owner	The agency official responsible for the development, procurement, integration, modification, operation and maintenance, and/or final disposition of an information system.
Technical Controls	The security controls for an information system that are primarily implemented and executed by the information system through mechanisms contained in system hardware, software, or firmware.
Two-Factor Authentication	Authentication can involve something the user knows (e.g., a password), something the user has (e.g., a smart card), or something the user "is" (e.g., a fingerprint or voice pattern). Single-factor authentication uses only one of the three forms of authentication, while two-factor authentication uses any two of the three forms. Three-factor authentication uses all three forms.
Unclassified Information	Information that has not been determined to be classified pursuant to Executive Order 13526, as amended
USB Device	A device that can be connected to a computer via a USB port.
USB Drive	A memory device small enough to fit into a pocket that connects to a computer via a USB port.
Vulnerability Scanning	An automated scan for potential security vulnerabilities.
Waiver	Temporary dispensation of a policy requirement, granted to a Component to operate a system while working toward compliance.

APPENDIX C REFERENCES

The DHS information security program and organization are based upon public laws, executive orders, national policy, external guidance, and internal DHS guidance.

Public Laws and U.S. Code

- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, DC, July 14, 1987
- *E-Government Act* of 2002, including Title III, *Federal Information Security Management Act (FISMA)*, 44 USC 3541
- Public Law 104-106, *Clinger-Cohen Act* of 1996, 40 U.S.C. 1401[formerly, Information Technology Management Reform Act (ITMRA)]
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*
- Public Law 100-235, *Computer Security Act of 1987 as amended*
- *Public Law 93-579, Freedom of Information Act* of 2002 as amended

Executive Orders

- Executive Order 13526, *Classified National Security Information*, December 29, 2009
- Homeland Security Presidential Directive 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004

Office of Management and Budget Directives

- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*
- OMB Bulletin 06-03, *Audit Requirements for Federal Financial Statements*
- OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information*, May 22, 2006
- OMB Memorandum M-06-16, *Protection of Sensitive Agency Information*, June 23, 2006
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007
- OMB Memorandum M-09-02, *Information Technology Management Structure and Governance Framework, October 21, 2008*
- OMB Memorandum 10-15, *FY 2010 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, April 21, 2010

- OMB Memorandum 10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS)*, July 6, 2010
- OMB Memorandum 11-06, *WikiLeaks - Mishandling of Classified Information*, November 28, 2010

Other External Guidance

- Intelligence Community Directive Number 508, *Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation*, September 15, 2008
- National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS), including:
  - NIST FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
  - NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- NIST Information Technology Security Special Publications (SP) 800 series, including:
  - NIST SP 800-16, Rev 1, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (Draft)
  - NIST SP 800-34, Rev 1, *Contingency Planning Guide for Information Technology Systems*
  - NIST SP 800-37, Rev 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*
  - NIST SP 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View* (Draft)
  - NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*
  - NIST SP 800-52, *Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations*
  - NIST SP 800-53, Rev 3, *Recommended Security Controls for Federal Information Systems and Organizations*
  - NIST SP 800-53A, Rev 1, *Guide for Assessing the Security Controls in Federal Information Systems*
  - NIST SP 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories: (2 Volumes) - Volume 1: Guide Volume 2: Appendices*
  - NIST SP 800-63, Rev 1, *Electronic Authentication Guideline* (Draft)
  - NIST SP 800- 65, Rev 1, *Recommendations for Integrating Information Security into the Capital Planning and Investment Control Process (CPIC) (Draft)*

- NIST SP 800-88, *Guidelines for Media Sanitization*
- NIST SP 800-92, *Guide to Computer Security Log Management*
- NIST SP 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*
- NIST SP 800-95, *Guide to Secure Web Services*
- NIST SP 800-100, *Information Security Handbook: A Guide for Manager*
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*
- NIST SP 800-118, *Guide to Enterprise Password Management* (Draft)
- *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NIST SP 800-123, *Guide to General Server Security*
- NIST SP 800-124, *Guidelines on Cell Phone and PDA Security*
- NIST SP 800-128, *Guide for Security Configuration Management of Information Systems* (Draft)
- NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations* (Draft)

- NIST IR 7298, *Glossary of Key Information Security Terms*
- CNSS Instruction No. 4009, *National Information Assurance Glossary*
- CNSS Instruction No. 1001, *National Instruction on Classified Information Spillage*

Internal Guidance

- Department of Homeland Security Acquisition Regulation (HSAR)
- DHS Management Directives (MD), especially:
  - MD 140-01, *Information Technology Systems Security*
  - MD 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*
  - MD 102-01 *Acquisition Management*
  - MD 1030, *Corrective Action Plans*
  - MD 4400.1, *DHS Web and Information Systems*
  - MD 4500.1, *DHS Email Usage*
  - MD 4600.1, *Personal Use of Government Office Equipment*
  - MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*
  - MD 11055, *Suitability Screening Requirements for Contractor Employees*

APPENDIX D DOCUMENT CHANGE HISTORY

Version	Date	Description
0.1	December 13, 2002	Draft Baseline Release
0.2	December 30, 2002	Revised Draft
0.5	January 27, 2003	Day One Interim Policy
1.0	June 1, 2003	Department Policy
1.1	December 3, 2003	Updated Department Policy
2.0	March 31, 2004	Content Update
2.1	July 26, 2004	Content Update
2.2	February 28, 2005	Content Update
2.3	March 7, 2005	Content Update
3.0	March 31, 2005	Includes updates to PKI, Wireless Communications, and Media Sanitization (now Media Reuse and Disposition) sections
3.1	July 29, 2005	New policies: 3.1b,e,f, 3.1g. 4.1.5b, 4.8.4a. Modified policies: 3.7b, e, 3.9b,g, 3.10a, 4.3.1b, 4.8.2a, 4.8.5e, 5.1.1b, 5.2.2a, 5.3a, c, 5.4.1a, 5.4.5d, 5.4.8c, 5.5.1a, 5.7d. Policies relating to media disposal incorporated into policies within Media Reuse and Disposition section. Deleted policy regarding use of automated DHS tool for conducting vulnerability assessments.
3.2	October 1, 2005	Modified policies 3.8b, 4.8.1a, 5.2.1a&b, 5.2.2a, and 5.4.3c; combined (with modifications) policies 4.1e and 4.1f; modified Section 1.5
3.3	December 30, 2005	New policies: policies 3.9a–d; 3.11.1b; 4.3.1a; 4.6c; 5.4.3d&e. Modified policies: policies 3.9i&j; 4.3.2a; 4.6a, b; 4.6.1c; 4.6.2j; 4.6.2.1a; 4.6.3e; 5.4.3c; 5.5.2k. Modified sections: 2.5, 2.7, 2.9, 2.11, 3.9, 5.5.2.
4.0	June 1, 2006	New policies: 3.5.3.c&g, 4.6.2.3.c, 5.1.c, 5.2.c, 5.4.1.a. Modified policies: 3.5.1.c, 3.5.3.d–f, 3.7.a&b, 3.9.a&b, d, 4.1.4.b&c, 4.2.1.a, 4.3.1.a, 4.6.c, 4.6.1.a, 4.6.2.f, 4.10.3.a, 5.2.1.b, 5.3.a&b, 5.4.1.b, 5.4.3.c, 5.4.5.d. Modified section: Section 2.9.
4.1	September 8, 2006	New policies: 3.14.1.a–c; 3.14.3.a–c; 4.10.1.c; 5.3.d&e; 5.4.1.c–e. Modified policies: 3.9.b; 4.6.2.d; 4.8.2.a–c; 4.10.1.b; 5.1.c; 5.3.c; 5.4.1.b. New sections: 3.14, 3.14.1, 3.14.3. Modified sections: 2.9, 4.8.2.
4.2	September 29, 2006	New policies: 4.6.4.a–f. Modified policies: 4.3.3.a–c. New section: 4.6.4.

Version	Date	Description
5.0	March 1, 2007	New policies: 4.1.5.h. Modified policies: 3.10.c, 4.1.1.d, 4.1.5.a,b,f, &g, 4.6.2.d, 4.6.3.f, 5.2.c, 5.4.8.a, 5.6.b. New sections: 4.1.1. Modified sections: 1.2, 1.4.2, 1.4.3, 2.9, 3.12, 4.1 and subsections, 4.6.1–4.6.4, 4.9, 5.2.1. Renumbered sections: 4.1.2-4.1.6, 4.9, 4.10, 4.11, 4.12.
5.1	April 18, 2007	Update based on SOC CONOPS. Final Version 1.4.1, April 6, 2007; Adds DHS Chief Financial Officer – Designated Financial Systems; Updates the term, *Sensitive But Unclassified* to *For Official Use Only*
5.2	June 1, 2007	Updates Sections 2.7, 2.9, 2.12, 3.3, 3.5.1, 3.5.3, 3.6, 3.8, 3.9, 3.10, 3.14, 3.15, 4.1.5, 4.1.6, 4.10, 4.12, 5.1.1, 5.2, 5.3, 5.4.1, 5.4.3, 5.4.4, 5.4.8, 5.5.1, 5.7
5.3	August 3, 2007	Revised policy in Sections 3.5.1 and 5.5.1, and removed Section 3.5.2. Removed Sections 3.11.2 and 3.11.4
5.4	October 1, 2007	Content update, incorporation of change requests
5.5	September 30, 2007	**Section 1.0:** 1.1 – Added text regarding policy implementation and DHS security compliance tool updates. 1.2 – Removed two references from list; deleted "various" from citation of standards. **Section 2.0:** 2.0 – Insert the following after the first sentence in the second paragraph: "Security is an inherently governmental responsibility. Contractors and other sources may assist in the performance of security functions, but a government individual must always be designated as the responsible agent for all security requirements and functions." 2.3 – Removed parentheses from "in writing." **Section 3.0:** 3.9 – Inserted new policy element "l" regarding CISO concurrence for accreditation. 3.15 – Added text regarding Component CFOs and ISSMs. **Section 4.0:** 4.1.1 – Capitalized "Background," and added "(BI)." 4.3.1 – Two new elements were added to the policy table. 4.7 – Inserted "where required or appropriate" before the sentence. 4.8.3 – Title changed to "Personally Owned Equipment and Software (not owned by or contracted for by the Government)." 4.8.6 – Included new section regarding wireless settings for peripheral equipment. **Section 5.0:** 5.1c – Changed inactive accounts to "disable user identifiers after forty-five (45) days of inactivity." 5.1.1 – First sentence of the second paragraph was rewritten to prohibit use of personal passwords by multiple individuals. 5.2.2 – Title changed to "Automatic Session Termination."
6.0	May 14, 2008	**Global change** "Shoulds" changed to "shalls" throughout the document. Replaced certain instances of "will" with "shall" throughout document to indicate compliance is required. Various changes were made throughout the document to ensure that the 4300A Policy and Handbook align with the 4300B Policy and Handbook. "ISSM" changed to "CISO/ISSM" throughout the document.

Version	Date	Description
		"CPO" changed to "Chief Privacy Officer" throughout the document. "IT Security Program" changed to "Information Security Program" throughout the document." "System Development Life Cycle" changed to "System Life Cycle" and "SDLC" changed to "SLC" throughout the document. **Title Page** Title page of 4300A Policy - Language on the Title Page was reworded. "This is the implementation of DHS Management Directive 4300.1." **Section 1.0** 1.1 – Updated to clarify 90 day period in which to implement new policy elements. 1.2 – Added OMB, NIST, and CNSS references. 1.4 – Added reference and link to Privacy Incident Handling Guidance and the Privacy Compliance documentation. 1.4.2 – Added definition of National Intelligence Information. 1.4.3 – Inserted definition of National Security Information to align with 4300B Policy. 1.4.8.1 – Definition of General Support System was updated. 1.4.8.2 – Definition of Major Application was updated. 1.4.10 – Section was renamed "Trust Zone." 1.4.16 – Inserted new definition for FISMA. 1.5 – Language was updated to increase clarity for financial system owners for waivers and exceptions. **Section 2.0** 2.3 – Added a new responsibility for DHS Chief Information Officer (CIO). 2.4 – Added a new responsibility for Component CIOs. 2.5 - Chief Information Security Officer (CISO) renamed DHS Chief Information Security Officer (CISO). Updated to include privacy-related responsibilities. 2.6 – Added a new section in Roles and Responsibilities called "Component CISO." 2.7 – Updated Component ISSM Role and Responsibilities. 2.8 – Changed name of the section from "Office of the Chief Privacy Officer (CPO)" to "The Chief Privacy Officer". Updated to include privacy-related responsibilities. 2.9 – Added a new role for DHS CSO. 2.10 – Updated to include privacy-related responsibilities. 2.11 - Added privacy-related responsibilities. 2.12 – Added a new section, "OneNet Steward."

Version	Date	Description
		2.13 – Added a new section, "DHS Security Operations Center (DHS SOC) and Computer Security Incident Response Center (CSIRC)."
		2.14 – Added a new section, "Homeland Secure Data Network (HSDN) Security Operations Center (SOC)."
		2.16 – Added a new section, "Component-level SOC."
		2.18 – Updated to include privacy-related responsibilities.
		2.19 – Last sentence of first paragraph has been updated to say: "ISSO Duties shall not be assigned as a collateral duty. Any collateral duties shall not interfere with their ISSO duties."
		2.20 – Updated to include privacy-related responsibilities.
		Section 3.0
		3.9 – Added C&A information for unclassified, collateral classified and SCI systems. Also, prior to DHS Policy table, included sentence regarding C&A.
		3.9.b – Language updated to clarify that a minimum impact level of moderate is required for confidentiality for CFO designated financial systems.
		3.9.h – New guidance is provided to clarify short term ATO authority.
		3.11.1 – Added new section discussing the CISO Board.
		3.11.3 – Removed DHS Wireless Security Working Group.
		3.14.1 – Added new text defining PII and sensitive PII. At the end of bullet #4, added definition of computer-readable data extracts. Updated 3.14.1.a and 3.14.1.b based on input from the Privacy Office. Added sentence "DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
		3.14.2 - Added new section called "Privacy Threshold Analyses."
		3.14.3 - Updated Privacy Impact Assessment Responsibilities table.
		3.14.4 - Added new section called "System of Record Notices."
		Section 4.0
		4.1.5.c – Updated to address training requirements.
		4.1.5.g – Deleted "Training plans shall include awareness of internal threats and basic IT security practices."
		4.1.5.h (now 4.1.5.g) – Updated to include the following sentence: "Components shall account for Contingency Plan Training, and Incident Response Training conducted for Moderate and High IT Systems."
		4.3.1.d – FIPS 140-2 compliance language was updated.
		4.8.1.a and 4.8.1.c – Language has been updated to provide clarification of timeout values.
		4.8.2.a – FIPS 140-2 compliance language was updated.
		4.8.2.b – Added a new policy element regarding powering down laptops

Version	Date	Description
		when not in use. 4.9 – Section was renamed "Department Information Security Operations." 4.9, 4.9.1, 4.9.2 – Updated policy elements to support Department security operations capabilities, based on the SOC CONOPS. 4.9.2.b – Updated to say "Components shall obtain guidance from the DHS SOC before contacting local law enforcement except where there is risk to life, limb, or destruction of property." 4.12.a – Added policy element to align with Handbook. **Section 5.0** 5.2.1.a, 5.2.1.b, and 5.2.1.c – Language has been updated to provide clarification of timeout values. 5.2.2 Introductory language, 5.2.2.a, 5.2.2.b, and 5.2.2.c – Language and policy updated to clarify the meaning of a session termination. 5.3.f - Updated to clarify responsibilities of the System Owner regarding computer-readable data extracts. 5.4.1.d – Added sentence "DHS has an immediate goal that remote access should only be allowed with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access." 5.4.3.a through i – New guidance is provided regarding the preparation of ISAs for interconnections to the DHS OneNetwork. 5.4.3.g – Replaced "interconnect service agreements" with "interconnection security agreements." 5.4.4.f - New guidance is provided regarding internal firewalls. 5.4.5.f – New guidance is provided regarding the use of the RDP protocol. 5.4.6 – Added text "NOTE: Due to many attacks that are HTML-based, please note that DHS will be following the lead of the DoD and moving to text based email." 5.4.8.a – Language updated to reflect that annual vulnerability assessments should be conducted. 5.4.8.f – Policy updated to clarify automated system scanning. 5.5.1.c – Updated element to specify usage of cryptographic modules that "are FIPS 197 compliant and have received FIPS 140-2 validation." 5.5.2.f – Policy updated to clarify hosting of DHS Root CA.
6.1	September 23, 2008	**Global Changes** Replaced all instances of "CISO/ISSM" with "Component CISO/ISSM." Replaced all DHS-related instances of "agency/agency-wide" with "Department/Department-wide." Replaced all instances of "24x7" with "continuous" or "continuously," as appropriate. Replaced all instances of "IT security" with "information security." Various minor editorial and grammatical changes were made throughout the

Version	Date	Description
		document. **Section 1.0** 1.2 – Added reference to E-Government Act of 2002, January 7, 2003. 1.4 – Replaced "National InfoSec Glossary" with "National Information Assurance (IA) Glossary." 1.4.5 – Replaced third sentence with "System vulnerability information about a financial system shall be considered Sensitive Financial Information." 1.5.2 – Added text regarding acceptance of resulting risk by the Component CFO for financial systems. 1.5.3 – Corrected the title and location of Attachment B. Added text regarding PTA requirements. **Section 2.0** 2.1 – Updated to clarify Secretary of Homeland Security responsibilities. 2.2 – Updated to clarify Undersecretaries and Heads of DHS Components responsibilities. 2.3 – Updated to clarify DHS CIO responsibilities. 2.4 – Updated to clarify Component CIO responsibilities. 2.5 – Updated to clarify DHS CISO responsibilities. 2.6 – Updated to clarify Component CISO responsibilities. 2.8 – Moved "The Chief Privacy Officer" section to 2.9. 2.11 – Updated to clarify Program Managers' responsibilities. 2.14 – Updated to clarify HSDN SOC responsibilities. Updated HSDN SOC unclassified email address. 2.19 – Updated to clarify ISSO responsibilities and the assignment of ISSO duties as a collateral duty. 2.20 – Updated to clarify System Owners' responsibilities. 2.23.2 – Updated to clarify DHS CIO responsibilities for financial systems. **Section 3.0** 3.1.e – Replaced "FISMA and OMB requirements" with "FISMA, OMB, and other Federal requirements." 3.1.h – Replaced "maintain a waiver" with "maintain a waiver or exception." 3.14.1 – Included text regarding the type of encryption needed for laptops. 3.14.3 – Included text stating that the PTA determines whether a PIA is conducted. 3.14.4 – Moved first sentence of second paragraph to be the first sentence of the first paragraph. Included "that are a system of record" after "IT Systems" in the second sentence of the first paragraph. **Section 4.0**

Version	Date	Description
		4.3.1.a – Included "locked tape device" in media protection.
		4.3.1.d – Updated to clarify that AES 256-bit encryption is mandatory.
		4.8.2.a – Updated to clarify that AES 256-bit encryption is mandatory.
		4.8.3.c – Included new policy element regarding use of seized IT equipment.
		4.8.4.f – Included new policy element regarding management and maintenance of system libraries.
		4.8.5.b – Policy updated to clarify limited personal use of DHS email and Internet resources.
		4.9 – First paragraph updated to clarify DHS SOC and HSDN SOC responsibilities.
		4.9.b – Updated to specify that the HSDN SOC is subordinate to the DHS SOC.
		4.9.1 – First two paragraphs updated to clarify relationship between the DHS SOC and the HSDN SOC.
		4.9.1.a – Removed the words "Component SOC."
		4.9.1.b – Updated to clarify means of communication for reporting significant incidents.
		4.9.1.c – Updated to clarify the length of time by which significant HSDN incidents must be reported.
		4.9.1.d. – Updated to clarify reporting for HSDN incidents.
		Section 5.0
		5.2.d – Replaced "Component CISO/ISSM" with "Component CISO/ISSM or his/her designee."
		5.2.1 – Changed "48 hour time period" to "24 hour time period."
		5.4.5.g – Included new policy element regarding blocking of specific Internet websitewebsitewebsites or categories.
		5.4.7 – Updated the policy element to prohibit use of Webmail and other personal email accounts.
		5.5.1.c – Updated to clarify that AES 256-bit encryption is mandatory.
		5.7.d – Included new policy element regarding use of cryptographic modules in order to align with 4300A Handbook.
		5.7.e – Included new policy element regarding rollback and journaling for transaction-based systems.
6.1.1	October 31, 2008	5.2.3 – Included new language and a link to the DHS computer login warning banner text on DHS Online.
7.0	July 31, 2009	**General Updates**
		Added section and reference numbers to policy elements
		Added NIST 800-53 reference controls to policy elements
		Added hyperlinks to most DHS references
		Introduced new terminology Senior Agency Information Security Officer,

Version	Date	Description
		Risk Executive, and Authorizing Official (AO) – replaces DAA, as per NIST 800-37 and 800-53 Added Appendix A – Acronyms Added Appendix B – Glossary Added Appendix C – References list has been updated and moved to Appendix C. (these are detailed references, an abbreviated list is still found at the beginning of the document) Added Appendix D – Change History (This was moved from the front of the document) **Specific Updates** **Section 1.1 – Information Security Program Policy** – Added the statement, "Policy elements are designed to be broad in scope. Specific implementation information can often be found in specific National Institute for Standards and Technology (NIST) publications, such as NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Systems." **Section 1.4.17-19 – Privacy** – Added definitions for PII, SPII, and Privacy Sensitive Systems **Section 1.5 – Exceptions and Waivers** – Updated this section, clarified policy elements, and consolidated all exceptions and waivers requirements. **Section 1.5.4 – U.S. Citizen Exception Requests** – Updated section to include policy elements: 1.5.4.a – Persons of dual citizenship, where one of the citizenships includes U.S. Citizenship, shall be treated as U.S. Citizens for the purposes of this directive. 1.5.4.b – Additional compensating controls shall be maintained for foreign nationals, based on nations lists maintained by the DHS CSO. **Section 1.6 – Information Sharing and Communication Strategy** – Added policy element: 1.6.a - For DHS purposes, electronic signatures are preferred to pen and ink or facsimile signatures in all cases except where pen & ink signatures are required by public law, Executive Order, or other agency requirements. **Section 1.7 – Changes to Policy** – Updated entire section **Section 2.0 – Roles and Responsibilities** – Reformats entire section. Places emphasis on DHS CISO and Component-level Information Security Roles. Secretary and senior management roles are moved to the end of the section. Some specific areas to note include: **Section 2.1.1 – DHS Senior Agency Information Security Officer** – Introduces this term and assigns duties to DHS CISO **Section 2.1.2 – Chief Information Security Officer** – Adds the following responsibilities: - Appoint a DHS employee to serve as the Headquarters CISO - Appoint a DHS employee to serve as the National Security Systems (NSS) CISO

Version	Date	Description
		Section 2.1.3 – Component Chief Information Security Officer – Adds policy element: 2.1.3.b - All Components shall be responsible to the appropriate CISO. Components without a fulltime CISO shall be responsible to the HQ CISO. Adds 4 additional CISOs to the list of Component CISOs: Federal Law Enforcement Training Center Office of the Inspector General Headquarters, Department of Homeland Security The DHS CISO shall also appoint an NSS CISO **Section 2.1.4 – Component Information Systems Security Manager –** Component CISO now works directly with the HQ CISO, rather than with the DHS CISO. **Section 2.1.5 – Risk Executive –** Introduces this term as per NIST. Assigns responsibilities to CISOs (already performing these functions) **Section 2.1.6 – Authorizing Official –** Introduces this term as per NIST. Replaces the term Designated Approval Authority (DAA) **Section 2.2.10 – DHS Employees, Contractors, and Vendors** – Adds the requirement for vendors to follow DHS Information Security Policy **Section 3.2 – Capital Planning and Investment Control** – Adds policy element: 3.2.f – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.3 – Contractors and Outsourced Operations** – Adds policy element: 3.3.g – Procurement authorities throughout DHS shall ensure that Homeland Security Acquisition Regulation (HSAR) provisions are fully enforced. **Section 3.5.2 – Contingency Planning** – Updates and expands entire section. **Section 3.7 – Configuration Management** – Adds policy elements Section 3.7.f – If the information system uses operating systems or applications that do not have hardening or do not follow configuration guidance from the DHS CISO, the System Owner shall request an exception, including a proposed alternative secure configuration. Section 3.7.g – Components shall ensure that CM processes under their purview include and consider the results of a security impact analysis when considering proposed changes. **Section 3.9 – Certification, Accreditation, and Security Assessments** – Updates entire section **Section 3.11.1 – CISO Council** – Updates the term from CISO Board **Section 3.14-3.14.6 – Privacy Sections** – Updates all sections pertaining to privacy and privacy information, adds section 3.14.5 – Protecting Privacy Sensitive Systems

Version	Date	Description
		Section 3.14.7 – E-Authentication – Renumbers this section from 3.14.6 (due to adding of privacy section 3.14.5 **Section 3.15 – DHS Chief Financial Officer Designated Systems** – Section renamed from DHS Chief Financial Officer Designated Financial Systems **Section 3.16 – Social Media** – Added Social Media section to provide guidelines and address the Federal Government's (including DHS) use of social media sites (You Tube, Twitter) **Section 4.1.2 – Rules of Behavior** – Added policy element: 4.1.2.b – Components shall ensure that DHS users are trained regarding rules of behavior and that each user signs a copy prior to being granted user accounts or access to information systems or data. **Section 4.1.5 – IT Security Awareness, Training, and Education** – Updates entire section **Section 4.1.6 – Separation from Duty** – Updates policy element to require that all assets and data are recovered from departing individuals 4.1.6.b – Components shall establish procedures to ensure that all DHS information system-related property and assets are recovered from the departing individual and that sensitive information stored on any media is transferred to an authorized individual. Adds policy elements: 4.1.6.c - Accounts for personnel on extended absences shall be temporarily suspended. 4.1.6.d – System Owners shall review information system accounts supporting their programs at least annually. **Section 4.3.2 – Media Marking and Transport** – Adds "Transport" to section title and adds policy element: 4.3.2.b – Components shall control the transport of information system media containing sensitive data, outside of controlled areas and restrict the pickup, receipt, transfer, and delivery to authorized personnel. **Section 4.6 – Wireless Network Communications** – Updated section title from "Wireless Communication" and specifies "network communication" technologies in policy, rather than the more general "Wireless." Removes references to the defunct "WMO." **Section 4.6.1 – Wireless Systems** – Adds policy elements: 4.6.1.f – Component CISOs shall review all system applications for wireless usage, maintain an inventory of systems, and provide that inventory to the DHS CISO at least annually. 4.6.1.g – Component CISOs shall (i) establish usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, and control wireless access to DHS information systems. **4.9.1 – Security Incidents and Incident Response and Reporting** – Adds requirement for Components to maintain full SOC and CSIRC capability (May outsource to DHS SOC). Adds policy elements:

Version	Date	Description
		4.9.1.k – Components shall maintain a full SOC and CSIRC capability or outsource this capability to the DHS SOC. The DHS SOC shall provide SOC and CSIRC services to Components in accordance with formal agreements. Information regarding incident response capability is available in Attachment F of the DHS 4300A Sensitive Systems Handbook. 4.9.1.q – The DHS CISO shall publish Incident Response Testing and Exercise scenarios as required. 4.9.1.r – The Component CISO for each Component providing an incident response capability shall ensure Incident Response Testing and Exercises are conducted annually in coordination with the DHS CISO. **Section 5.1 – Identification and Authentication** – Adds requirement for strong authentication following HSPD-12 implementation. 5.1.f – Components shall implement strong authentication on servers, for system administrators and significant security personnel, within six (6) months of the Component's implementation of HSPD-12. **Section 5.4.1 – Remote Access and Dial-In** – Updates section and adds policy element: 5.4.1.f – The Public Switched Telephone Network (PSTN) shall not be connected to OneNet at any time. **5.4.3 – Network Connectivity** – Requires DHS CIO approval for all network connections outside of DHS. Also specifies requirement for CCB. 5.4.3.g – The DHS CIO shall approve all interconnections between DHS information systems and non-DHS information systems. Components shall document interconnections with an ISA for each connection. The DHS CIO shall ensure that connections with other Federal Government Agencies are properly documented. A single ISA may be used for multiple connections provided that the security accreditation is the same for all connections covered by that ISA. 5.4.3.1 - The appropriate CCB shall ensure that documentation associated with an approved change to an information system is updated to reflect the appropriate baseline. DHS systems that interface with OneNet shall also be subject to the OneNet CCB. **Section 5.4.4 – Firewalls and Policy Enforcement Points** – Updates language to include Policy Enforcement Points. Adds policy elements: 5.4.4.i – The DHS CISO shall establish policy to block or allow traffic sources and destinations at the DHS TIC PEPs. The DHS CISO policy will prevent traffic as directed by the DHS CIO. 5.4.j – The DHS SOC shall oversee all enterprise PEPs. **Section 5.4.5 – Internet Security** – Prohibits Public Switched Telephone Network (PSTN) connection to OneNet. 5.4.5.a – Any direct connection of OneNet, DHS networks, or DHS mission systems to the Internet or to extranets shall occur through DHS Trusted Internet Connection (TIC) PEPSs. The PSTN shall not be connected to OneNet at any time. **Section 5.5.3 – Public Key/Private Key** – Assigns responsibility for non-

Version	Date	Description
		human use of PKI to sponsors. 5.5.3.g – Sponsors for non-human subscribers (organization, application, code-signing, or device) shall be responsible for the security of and use of the subscriber's private keys. Every sponsor shall read, understand, and sign a "DHS PKI Subscriber Agreement for Sponsors" as a pre-condition for receiving certificates from a DHS CA for the non-human subscriber. **Section 5.4.6 – Email Security** – Prohibits auto-forwarding of DHS email to other than .gov or .mil addresses. 5.4.6.i - Auto-forwarding or redirecting of DHS email to address outside of the .gov or .mil domain is prohibited and shall not be used. Users may manually forward individual messages after determining that the risk or consequences are low. **Section 5.4.7 – Personal Email Accounts** – Requires use of encryption when sending sensitive information to email addresses other than .gov or .mil addresses. 5.4.7.b - When sending email to an address outside of the .gov or .mil domain, users shall ensure that any sensitive information, particularly privacy data, is attached as an encrypted file. **Section 5.6 – Malware Protection** – Updates term from "Virus."
7.1	September 30, 2009	**General Updates** Standardized the term "IT system" to "information system" Standardized the term "DHS IT system" to "DHS information system" Updated the term "DHS Security Operations Center" to "DHS Enterprise Operations Center" and added definition in glossary Replaced "must" with "shall" in all policy statements Replaced "vendors" with "others working on behalf of DHS" **Specific Updates** **Section 1.4.20** – Strong Authentication – Added definition for Strong Authentication **Section 1.4.21** – Two-Factor Authentication – Added definition for Two-Factor Authentication **Section 2.2.4** – Component Chief Information Officer – Alleviated confusion regarding Component CIO responsibilities **Section 2.2.5** – Chief Security Office – Removed erroneous CSO responsibilities which belong to Component CIOs **Section 2.2.7** – DHS Chief Financial Officer – Updated policy elements to clarify applicable policies **Section 3.1** – Basic Requirements (3.1.d, 3.1.g-j) – Updated policy elements to CISO/ISSM/ISSO responsibilities **Section 3.7.f** – Clarified Operating system exception requirements **Section 3.9.1-m** – Clarified requirements regarding TAF/RMS **Section 3.15** – CFO Designated Systems – Major revisions to this section

Version	Date	Description
		Section 4.6.2 and 5.4.1.a – Prohibits tethering to DHS devices **Section 5.4.3.g-h** – Clarifies interconnection and ISA approval **Section 5.5** – Cryptography – Removed unnecessary elements from introductions and updated entire section with input from DHS PKI Steward
7.2	May 17, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.4.8** – Added FISMA language (transmits, stores, or processes data or information) to definition of DHS System **Section 1.5.3.k** – Removed requirement for Component Head to make recommendation regarding waivers; removed requirement to report *exceptions* on FISMA report. **Section 2.1.6** – Adds requirement for AO to be a Federal employee **Section 2.1.7** – Clarifies that CO is a senior management official; stipulates that CO must be a Federal employee **Section 2.2.5** – Updated CSO role **Section 3.2** – Added intro to CPIC section and link to CPIC Guide **Section 3.5.2.h** – Added requirement to coordinate CP and COOP testing moderate and high FIPS categorizations **Section 3.15.a** – Added requirement for CFO Designated Systems security assessments for key controls be tracked in TAF and adds requirement for tracking ST&E and SAR annually. **Section 3.15.c** – Remaps control from RA-4 to RA-5 **Section 3.15.h** – Adds mapping to IR-6 **Section 3.15.i** – Remaps control from PL-3 to PL-2 **Section 3.17** – Added requirement to protect HIPAA information **Section 4.1.1.a** – Added requirement for annual reviews of position sensitivity levels **Section 4.1.1.c** – Exempts active duty USCG and other personnel subject to UCMJ from background check requirements **Section 4.1.4.c-d** – Adds additional separation of duties requirements and restricts the use of administrator accounts **Section 5.2.f** – Limits the number of concurrent connections for FIPS-199 high systems **Section 5.4.2.a** – Limits network monitoring as per the Electronic Communications Act **Section 5.4.3** – Added introduction to clarify ISA requirements **Section 5.4.3.f** – Clarifies the term "security policy" in context **Section 5.4.3.m** – Clarifies that both AOs must accept risk for interconnected systems that do not require ISAs.

Version	Date	Description
		Section 5.4.3.m-n – Adds stipulations to ISA requirements **Section 5.5** – Updates language in entire section **Section 5.5.3.j** – Assigns the DHS PKI MA responsibility for maintaining Human Subscriber agreements
7.2.1	August 9, 2010	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 1.1** – Removes reference to 4300C **Section 1.4.1/3** – Updates Executive Order reference from 12958 to 13526 **Section 1.4.17** – Updates the PII section **Section 1.4.18** – Updates SPII section **Section 1.5.3** – Adds requirement for Privacy Officer/PPOC approval for exceptions and waivers pertaining to Privacy Designated Systems **Section 1.6.b/c** – Requires installation and use of digital signatures and certificates **Section 2.1.6.d** – Allows delegation of AO duty to review and approve administrators **Section 2.2.6** – Updates DHS Chief Privacy Officer description **Section 3.7.e** – Adds requirement to include DHS certificate as part of FDCC **Section 3.14** – Updates Privacy and Data Security section **Section 3.14.1** – Updates PII section **Section 3.14.2** – Updates PTA section **Section 3.14.2.e** – Updates impact level requirements for Privacy Sensitive Systems **Section 3.14.3** – Updates PIA section **Section 3.1.4.4** – Updates SORN section **Section 3.14.4.a** – Exempts SORN requirements **Section 3.14.5** – Updates Privacy Sensitive Systems protection requirements **Section 3.14.6.a** – Updates privacy incident reporting requirements **Section 3.14.7** – Updates privacy requirements for e-Auth **Section 3.14.7.e** – Adds PIA requirements for eAuth **Section 4.1.1.e** – Expands U.S. citizenship requirement for access to all DHS systems and networks **Section 4.1.4.b** – Allows delegation of AO duty to review and approve administrators **Section 4.6.2.3.c** – Clarifies prohibited use of SMS

Version	Date	Description
		Section 4.8.4.h – Updates the term "trusted" to "cleared" maintenance personnel **Section 4.12.i** – Updates escort requirements for maintenance or disposal **Section 4.12.j** – Requires disabling of dial up on multifunction devices **Section 5.4.3** – Clarifies definition of Network Connectivity **Section 5.4.3.m/n** – Clarifies requirement for ISA **Section 5.4.6.j** – Requires DHS email systems to use a common naming convention **Section 5.5.3.g** – Prohibits sharing of personal private keys
7.2.1.1	January 19, 2011	**General Updates** No general updates with this revision. Specific updates are listed below. **Specific Updates** **Section 4.8.1.a** – Changes requirement for screensaver activation from five (5) to fifteen (15) minutes of inactivity.
8.0	March 14, 2011	**General Updates** Update date and version number Replace "certification and accreditation" and "C&A" with "security authorization process". Replace "Certifying Official" with "Security Control Assessor". **Replace "ST&E Plan" with "security control assessment plan".** **Replace "ST&E" with "security control assessment"** Replace "system security plan" with "security plan" and "SSP" with "SP". **Specific Updates** **Section 1.4.8.1:** Change definition to specify that a GSS has only one ISSO. **Section 1.4.8.2:** Change definition to specify that an MA has only one ISSO. **Section 1.5.1:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.2:** Include language requiring waiver submissions to be coordinated with the AO. **Section 1.5.3:** Clarify language regarding submission of waivers and exceptions for CFO designated systems. **Section 1.6.d:** Added new policy element, "DHS and Component systems shall be able to verify PIV credentials issued by other Federal agencies." **Section 2.1.2:** Add DHS CISO role as primary liaison to Component officials, and to perform periodic compliance reviews for selected systems. **Section 2.13:** Update Component CISO duties and add to implement POA&M process and ensure that eternal providers who operate information

Version	Date	Description
		systems meet the same security requirements as the Component. **Section 2.1.4:** Update list of Component ISSM duties and create a POA&M for each known vulnerability. **Section 2.1.5:** Add significantly expanded Risk Executive duties. **Section 2.1.6:** Add significantly expanded Authorizing Official duties. **Section 2.2.8:** Add Program Manager responsibility for POA&M content. **Section 2.2.9:** Add expanded System Owner duties. **Section 2.2.11:** Renumber 2.2.10 as 2.2.11. **Section 2.2.10:** Add a new 2.2.10 to introduce and describe duties of Common Control Provider. **Section 3.2.g:** Added new policy element, "Procurements for services and products involving facility or system access control shall be in accordance with the DHS guidance regarding HSPD-12 implementation." **Section 3.5.2.c:** Updated language to clarify requirements for backup policy and procedures. **Section 3.5.2.f:** Updated language to require table-top exercises for testing the CP for moderate availability systems. **Section 3.7.f:** Added new policy element, "Components shall monitor USGCB (or DHS-approved USGCB variant) compliance using a NIST-validated Security Content Automation Protocol (SCAP) tool." **Section 3.9:** Add requirement for Components to designate a Common Control Provider. **Section 3.10.b:** Policy element language was updated to clarify the function of information system security review and assistance programs. **Section 3.14:** Language updated for readability. **Section 3.14.c:** Added new policy element, "Components shall review and republish SORNs every two (2) years as required by OMB A-130." **Section 3.14.7.f:** Added new policy element, "Existing physical and logical access control systems shall be upgraded to use PIV credentials, in accordance with NIST and DHS guidelines." **Section 3.14.7.g:** Added new policy element, "All new systems under development shall be enabled to use PIV credentials, in accordance with NIST and DHS guidelines, prior to being made operational." **Section 3.17:** Added reference to NIST SP 800-66 for more information on HIPAA. **Section 4.1.4.d:** Language updated to clarify usage of administrator accounts. **Section 4.1.5.f:** Language updated to clarify requirements for security awareness training plan. **Section 4.3.1.b:** Language updated to clarify protection of offsite backup media.

Version	Date	Description
		Section 4.5.4: Added reference to NIST SP 800-58 for more information on VoIP. **Section 4.9.j:** Language updated to require that Component SOCs report operationally to the respective Component CISO. **Section 4.9.k:** New policy element added, "The DHS EOC shall report operationally to the DHS CISO." **Section 4.10:** Revise list of annual system documentation updates. **Section 4.12.c:** Policy element replaced with new one stating that the policy applies "to all DHS employees, contractors, detailees, others working on behalf of DHS, and users of DHS information systems that collect, generate, process, store, display, transmit, or receive DHS data." **Section 5.4.1.e:** Policy element removed. **Section 5.4.1.f:** Policy element removed. **Appendix A:** Include new acronyms **Appendix B:** Revise definition of Accreditation Package to reflect new list of documentation. **Appendix C:** Update references
9.0	October 11, 2011	**General Updates** Various minor grammatical and punctuation changes were made throughout the document. **Specific Updates** **Section 1.5.3.a:** New policy element added to state that the 4300A Policy and Handbook apply to all DHS systems unless a waiver or exception has been granted. **Section 2.1.3:** NPPD added to the list of Components having a fulltime CISO. **Section 2.1.8.g:** New policy element added to ensure ISSO responsibility for responding to ICCB change request packages. **Section 3.14.7.e:** Policy element revised to require consultation with a privacy officer to determine if a change requires an updated PTA. **Section 3.14.7.h:** New policy element added to ensure that all new DHS information systems or those undergoing major upgrades shall use or support DHS PIV credentials. **Section 4.1.5.d:** Policy element revised to clarify awareness training records requirements. **Section 4.1.5.e:** Policy element revised to clarify role-based training records requirements. **Section 4.1.5.g:** Policy element revised to require submission of an annual role-based training plan. **Section 4.1.5.j:** Policy element revised to require annual DHS CISO review of role-based training programs.

Version	Date	Description
		Section 4.1.5.k: Policy element revised to require biannual submission of roster of significant information security personnel and to specify the standard information security roles. **Section 4.3.1.f:** Policy element prohibiting connection of DHS removable media to non-DHS systems. It was already stated in 4.3.1.e. **Section 4.12.c:** Policy element was moved to 1.5.3.a. **Section 5.2.f:** Policy element revised to allow concurrent sessions to one if strong authentication is used. **Section 5.2.g:** New policy element added to ensure preservation of identification and access requirements for all data-at-rest.
9.0.1	March 5, 2012	**Section 2.1.3:** Includes language to address the designation of a Deputy CISO by the Component CISO. Add two new responsibilities for Component CISO: Serve as principal advisor on information security matters; Report to the Component CIO on matters relating to the security of Component information Systems. **Section 2.2.4:** Includes new language stating that the Component CISO reports directly to the Component CIO. **Section 4.1.1.c:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to Federal employees. **Section 4.1.1.d:** Includes new language to give Components the option to use background investigations completed by another Federal agency when granting system access to contractor personnel.
9.0.2	March 19, 2012	**Section 1.6:** Section 1.6, Information Sharing and Electronic Signature was divided into two sections – Section 1.6, Electronic Signatures, and Section 1.7, Information Sharing. **Section 1.8:** Section 1.8, Threats, was added to the policy. **Section 3.9.w:** Policy element added to require common control catalogs for DHS enterprise services. **Section 3.9.x:** Policy element added to require the development of Enterprise System Security Agreements for enterprise services. **Section 5.1.g:** Policy element added to require use of PIV credentials for logical authentication where available.

Question#:	13
Topic:	RSA
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: In 2011, RSA, a leading cyber security firm, was victimized by a cyber attack, which potentially exposed federal networks. Can you please describe the actions that DHS took in response to that incident?

Response: On March 11, 2011, a third party notified the Department of Homeland Security (DHS) about a significant cyber intrusion and data theft at RSA, a leading identity and access management vendor. Federal Bureau of Investigation (FBI), National Security Agency (NSA), and the DHS United States Computer Emergency Readiness Team (US-CERT) personnel provided technical assistance to RSA as the company formulated its initial response to the incident. On March 17, 2011, RSA released a security breach notification detailing the attacks that had affected the company's SecurID authentication products.

DHS assisted in developing mitigation strategies for RSA and for organizations within the U.S. Government and Critical Infrastructure sectors that could be potentially affected by the data theft. DHS worked with RSA leadership and established trusted communication channels to coordinate DHS and RSA product releases. The National Cyber Security Division's Federal Network Security branch hosted a briefing on the RSA breach and mitigation actions for the Chief Information Officers and Chief Information Security Officers of Scorecard departments and agencies. US-CERT and National Cybersecurity and Communications Integration Center (NCCIC) staff provided information on the compromise and the potential threat to federal systems. Following is a timeline of actions that US-CERT took in response to the RSA incident:

- March 11, 2011
  - submitted requests for information to inter agency partners at the unclassified-level and gathered information on adversarial tactics, techniques, and procedures;
  - recommended that organizations re-evaluate and institute recommended best practices with regards to this compromise;
  - posted a Technical Information Paper on system integrity on www.US-CERT.gov;
  - sent a US-CERT Advisory draft document to the NCCIC's Cyber Unified Coordination Group (UCG). They then released the US-CERT Advisory hard copy at the 1500 CIO/CISCO briefing and posted it to the US-CERT Portal's Government Forum of Incident Response (GFIRST).

Question#:	13
Topic:	RSA
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

- recommended that industry subject matter experts form an Incident Management Team sub- working group under the Critical Infrastructure Partnership Advisory Council to develop a mitigation plan for this type of incident.

- March 18, 2011
  - created a Leadership Awareness Notice;
  - developed an Incident Action Plan that included mitigation steps through the Cyber UCG. A sanitized version was also created for the general public; and
  - released Technical Information Paper (TIP) 11-075-01 System Integrity Best Practices, which was distributed to Critical Infrastructure and Usual Five trusted partners and is also available on the US-CERT Public Website at www.US-CERT.gov.
- March 19, 2011
  - posted Situation Awareness Report (SAR) 11-078-01, RSA Compromise, to GFIRST's Analysis and Informational Papers and to OMB's Situational Awareness Reports, and
  - posted SAR 11-161-01, Hardening of Authentication Strategies, to the GFIRST portal.

Question#:	14
Topic:	CFATS
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Since December, we have learned that DHS conducted an internal audit of the Chemical Security Anti-Terrorism Standards (CFATS) program. The audit found that DHS has failed to establish a successful chemical security program after 5-years. Can you please explain why we should have confidence that DHS will be better at handling cyber security than it has been at regulating and inspecting chemical facilities' security?

Response: The proposal in the Cybersecurity Act of 2012 (S. 2105) to ensure a baseline level of cybersecurity for the Nation's most critical infrastructure differs from the Chemical Security Anti-Terrorism Standards (CFATS) program in a number of ways The "light-touch" approach proposed by the Administration and S. 2105 represents a completely new way of approaching regulations that is much more flexible and collaborative. For example, the cybersecurity program will be based on standards developed by industry and companies can demonstrate compliance with the standards through self-certifications instead of requiring a DHS inspection.

The Department has identified a number of programmatic and management challenges in the CFATS program that we are working to remedy. Lessons learned from this process will certainly inform our efforts going forward.

Some areas of progress include the following:

• Hiring of staff: The Infrastructure Security Compliance Division (ICSD) is leading an internal analysis to determine the proper staffing needs of the Division and ensure that the CFATS workforce is qualified to meet those needs.

• Training of staff: ISCD is conducting a comprehensive review of the curriculum from the training courses ISCD previously provided to its Inspectors.

• How inspections are to be conducted: ISCD stood up a working group in September 2011 to review the current processes, procedures, and equipment utilized by the inspector cadre and to update or develop additional materials and tools to further assist the inspector cadre in performing future authorization inspections as well as compliance inspections.

We believe that we are making progress to address the identified challenges as evidenced by the examples above, but we recognize that more work remains to be done. We continue to review the CFATS program and will use the lessons learned from standing up this unprecedented regulatory program to any cybersecurity regulatory authority we may receive from Congress.

Question#:	15
Topic:	compliance
Hearing:	Securing America's Future: The Cybersecurity Act of 2012
Primary:	The Honorable Tom A. Coburn
Committee:	HOMELAND SECURITY (SENATE)

Question: Is there a risk that the proposed regulatory approach to cyber security would have the unintended consequence of causing regulated entities to focus on compliance rather than innovating and developing solutions to minimize cyber vulnerabilities?

Response: The flexible risk-based performance requirements are specifically designed to enhance the existing public-private partnership that exists today between critical infrastructure owners and operators and the Department. The focus on performance outcomes—rather than any particular mandated standard or control—will promote the real and innovative security envisioned in the legislation. Any regulated critical infrastructure owner or operator will have the ability to adopt any measures that will allow them to achieve the performance requirements identified by the Department in accordance with Section 104. Owners and operators will not be able to simply select controls off a list, but will instead need to examine and evaluate their specific mission critical functions, systems, and assets, leading to much more dynamic security.

Post-Hearing Questions for the Record
Submitted to the Honorable Thomas J. Ridge
From Senator Tom Coburn

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

(1) Given your experience as the first Secretary of Homeland Security, do you believe that the Department of Homeland Security has the expertise to oversee and regulate cyber security for the federal government and the private sector?

I have immense respect for the dedicated men and women who work for the Department of Homeland Security (DHS). Department leadership is working diligently to recruit and hire cybersecurity professionals to help fulfill DHS's broad mission to help protect the nation's cyber infrastructure, systems, and networks.

I agree with Homeland Security Secretary Napolitano, who testified that DHS is responsible for coordinating the national response to significant cyber incidents, consistent with the National Response Framework, and for creating and maintaining a common operational picture for cyberspace across the government. DHS also coordinates cybersecurity outreach and awareness efforts. The U.S. Chamber of Commerce has collaborated with DHS in raising the cyber education and awareness of both the general public and business community to create a more secure environment in which the personal or financial information of individuals is better protected.

However, the federal government, including DHS, should not be given new authorities by Congress to regulate cybersecurity for the private sector, not least because businesses already adhere to an array of information-security rules, ranging from chemical security to energy to financial. I will explain my reasons more fully in question number 3.

(2) Are you concerned about the DHS Inspector General's October 2010 audit, "DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems," that reported that US-CERT's own network has critical vulnerabilities?

Yes, the report is a concern. The United States Computer Emergency Readiness Team (US-CERT), the operational arm of DHS's National Cyber Security Division (NCSD), plays a vital role in compiling and analyzing information about cybersecurity incidents and providing technical assistance to government and business operators of information systems. I understand that since the report appeared, DHS has been taking actions to improve the physical and cybersecurity of US-CERT, consistent with the IG's recommendations.

Still, the report should highlight for policymakers that an increasingly sophisticated threat environment puts cybersecurity beyond the reach of any single organization, whether public or private. Government and the private sector must work together to mitigate risks to economic and national security.

The report also discusses the importance of adhering to the requirements under the Federal Information Security Management Act of 2002 (FISMA). The federal cybersecurity landscape has changed since FISMA was first enacted. There is a strong need to harmonize information security programs across civilian government agencies. A reformed FISMA would help the government shift from a snapshot-in-time approach to information security to one that continually monitors servers and computers for weaknesses. Above all, the government needs to lead by example and work toward securing its own computers and information systems before imposing new mandates on the private sector.

(3) In your testimony, you warned that a DHS cyber security regulatory program would likely become highly rigid in practice and counterproductive to effective cyber security. Please discuss this potential outcome in greater detail. Would regulations lead to a focus on compliance rather than the kind of innovations that are needed to respond to and prevent cyber attacks?

I testified that DHS should not be given new authorities to regulate the assets or systems of vital parts of the American economy. The Chamber believes that such discretion to decide which infrastructure should be "covered"—or regulated—is unreasonably broad. The Chamber is concerned both with the "covered" critical infrastructure (CCI) concept and how it would be implemented. A regulatory program would become highly prescriptive in practice and thus counterproductive to effective cybersecurity—due in large part to a shift in businesses' focus from security to compliance. Cybersecurity should not become a "check-the-box" exercise. For every new solution we put in place, the attackers are already seeking a means to circumvent a company's protections and similarly situated organizations.

Any proposed legislation must promote, not stifle, innovation. Threats are rapidly evolving and so must the technology to mitigate those threats. Our cyber adversaries are dynamic and increasingly sophisticated, and are not bound by red tape. The challenges we face in cybersecurity cannot be solved by imposing slow-moving, bureaucratic processes on those who build, operate in, and use cyberspace. Regulation and certification requirements will likely have unintended consequences, such as emphasizing the status quo by focusing on yesterday's threats. A prescriptive approach to cybersecurity would stifle the technology leadership of the United States in the global information and communications system.

Any cybersecurity innovation legislation must promote technology advancement so we can stay ahead of the curve. The Chamber has been a supporter of a national cybersecurity research and development (R&D) strategy. Cybersecurity policy should therefore maximize the ability of organizations to develop and adopt the widest possible choice of cutting-edge cybersecurity solutions. An effective way to do this is through spurring national cybersecurity R&D. The Chamber urges Congress to leverage existing public-private partnerships to create a cybersecurity R&D plan that supports national (not simply governmental) priorities and includes a realistic road map for implementation, such as how to transition the benefits of research into operational environments.

Organizations like the National Institute for Standards and Technology need to ensure the U.S. government's—as well as the private sector's, where appropriate—participation in the development of international cybersecurity standards and best practices. The Chamber also advocates increasing and making permanent the R&D tax credit, which can serve as a means of encouraging companies to increase their investments in cybersecurity.

Post-Hearing Questions for the Record
Submitted to the Honorable Stewart A. Baker
From Senator Tom Coburn

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

Question 1: In your testimony, you used the analogy that we are living in a digital New Orleans, and imply that we need to start reinforcing our levees. Can you please comment on what the federal government is currently spending on cyber security, and whether you think these investments are being spent effectively?

There is little doubt that cybersecurity is a sizeable line item on the federal budget and it is bound to grow. The Department of Homeland Security, for example has a FY 2012 cybersecurity budget of $443 million and has requested a nearly 74% increase for FY 2013.[1] These types of increases are necessary as we intensify efforts to protect government networks and as the government expands its role to helping ensure the security of the internet more broadly.

But that does not mean that there is no room for improvement in how the federal government spends its money now. Government spending on information technology is plagued by inefficiencies, and spending in the area of cybersecurity is no exception. This is due in part to the complexity of government contracting requirements. It is also largely due to the scattered nature of the IT procurement process, with each department left to make its own IT procurement decisions with regard to cybersecurity.

One way to improve matters would be to require greater standardization across departments. This should include increased reliance on standard commercial products. Many such products still carry heavy price tags, but they are often a more cost effective solution than relying on contractors to produce unique solutions for individual departments or agencies.

The challenge, of course, is creating rules to ensure that all departments maintain similar levels of cybersecurity, and to do that an agency like DHS must have the authority to enforce standard security requirements, including the ability to force agencies to make particular investments in security. Beating the current crop of state-sponsored attackers is not impossible, just expensive and somewhat inconvenient. Australia's Defence Signals Directorate, for example, maintains a list of 35 Strategies to Mitigate Targeted Cyber Intrusions.[2] If U.S. government agencies want to make state sponsored attacks less successful, DHS should adopt a list along those lines and then require all federal civilian departments to adopt the items on the list.

---

[1] Department of Homeland Security Annual Performance Report Fiscal Years 2011 – 2013 (DHS's FY 2013 Congressional Budget Justification), section covering Infrastructure Protection and Information Security, at 9.

[2] Strategies to Mitigate Targeted Cyber Intrusions, Defense Signals Directorate, http://www.dsd.gov.au/infosec/top-mitigations/top35mitigationstrategies-list.htm (last visited Mar. 15, 2012).

Question 2: Can you please comment on the DHS Inspector General's report that found that US-CERT's own network was vulnerable to cyber attacks? Should we be confident that the Department of Homeland Security will succeed in leading cyber security for the federal government and critical infrastructure?

A 2010 report published by the Office of Inspector General at DHS did indeed, among other things, find vulnerabilities within one of US-CERT's systems, its Mission Operating Environment ("MOE").[3] It also found, however, that three other US-CERT's systems were adequately protected, and the main concern the report cited regarding the MOE was a lack of effective software patching.[4]

It is regrettable (and embarrassing) that US-CERT did not get an A grade on its own internal security management procedures, but this is a separate issue from whether DHS is capable of playing a leading regulatory role in protecting our country's IT infrastructure. I don't think anyone expects the staff of the Federal Communications Commission to be able to run a local radio or television station; we expect the FCC to act as a competent regulator. In the same way, we should be looking to DHS's capabilities to play the role that the bills currently on the table propose to give it.

That said, I don't deny that when DHS was stood up in 2002, it inherited more responsibilities with respect to cybersecurity than personnel capable of handling them. And since then, DHS has struggled to compete with a booming cybersecurity market in the private sector.

But for all that, DHS is the best positioned department to play a leading role in securing civilian agencies and critical infrastructure. First, in the last four years, DHS has turned a corner in its cybersecurity hiring and has been putting in place a much more capable team. Second, there is no other civilian agency with remotely comparable cybersecurity abilities.

It is true that the National Security Agency has more experience and capable personnel on cybersecurity than DHS. I am an alumnus of both DHS and NSA, and with encouragement from me, NSA has been sharing its expertise with DHS for years; it will continue to do so. DHS will have to rely on NSA for some operational and technical cybersecurity capabilities for years, but when it comes to protecting our civilian infrastructure, I think most people want civilian leadership in charge of cybersecurity policy making. And DHS is the civilian agency most capable of playing that role.

---

[3] *DHS Needs to Improve the Security Posture of Its Cybersecurity Program Systems*, Office of Inspector General, Department of Homeland Security, OIG-10-11, at 7-10 (August 2010).

[4] *Id.*

Post-Hearing Questions for the Record
Submitted to James A. Lewis, Ph.D.
From Senator Tom Coburn

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

1. During the hearing, you stated that we should assume that all networks have been compromised. Can you please discuss this in greater detail?

One of the things we routinely hear about cybersecurity these days is that a "perimeter defense" approach is no longer adequate. The "perimeter" people are talking about when they say this is the border between their network and the internet. Perimeters are routinely breached and no one can safely assume that they can keep opponents out of their networks. This is why people now talk about "defense in depth," which is predicated on the notion that attackers have penetrated the network, gotten inside past the perimeter defenses, and that additional defensive measures (such as encrypting data or restricting access permissions) are needed. A secure perimeter is a dubious assumption and any defensive strategy that doesn't assume compromise is inadequate.

Intelligence officials say this is the "golden age" of cyber espionage because networks are so easy to compromise. Unfortunately, this is also true for our opponents, who have unparalleled access to US networks. These officials could also tell you that every network they examine appears to have been penetrated. DHS's ICS-CERT, responsible for industrial control systems, says that penetrations it has found lasted an average of eighteen months before being discovered.

There are simply too many examples of compromised networks to list. Google remains the most salient example. Google had the courage to admit to compromise, but we know that dozens of other companies, including many high tech companies, were hacked at the same time and simply denied the fact. The Nortel case, where the attacker sat on the company network for years before being discovered, is another example. All of these companies thought their networks were secure. They assumed they hadn't been compromised. They were wrong. The bottom line is that any network connected to the internet is at risk and that a sound defensive strategy should begin with the assumption that the network can be compromised.

2. Does this include federal agencies with sensitive networks and cyber security contractors providing services to the federal government?

The inadvertent result of a voluntary, uncoordinated approach to cybersecurity has been to create endless opportunities for America's opponents. Voluntary, uncoordinated actions are how amateurs approach national security. It never works against a serious opponent. We want to move from the amateur approach that has dominated cybersecurity for years to something more consistent with operational security and strategic thinking. In cyberspace, the opening assumption for defense should be that you cannot secure your perimeter. Two oceans may separate the U.S. from potential opponents but we learned in the last century that technology makes this separation an illusion for security. The internet only makes it easier to operate in the

U.S., primarily because as a nation, we have done far too little to secure our networks.

The best known instance of penetration of a sensitive network available in public sources is the 2008 penetration of the Department of Defense's SIPRNET classified network. You may want to ask Federal agencies to learn of other example that have not been made public. DOD's energetic response to the problem of the penetration of its classified military network included a range of actions, such as consolidating its cybersecurity efforts and in providing classified briefings to leading DOD contractors on the failure of network security at their companies. However, as DOD improved its own cyber defenses, opponent attention turned to contractors, who were a soft target by comparison. DOD then began work to improve contractor cybersecurity. You may wish to ask for a classified briefing on this effort and the losses of defense technology since 2000 to foreign cyber espionage efforts against contractor networks.

If we were to ask the administrators of sensitive networks, I would be surprised to find one who would say that he or she assumes that any network connected to the internet cannot be compromised. At this time, given the larger failure of cybersecurity, defense for any network should be based on the assumption that compromise is possible. We must plan accordingly. This is why FISMA reform is so important for improving the security of government networks - but there is now nothing like FISMA for the private sector.

3. Can you please comment on the DHS Inspector General's report that found that US-CERT's own network was vulnerable to cyber attacks? Should we be confident that the Department of Homeland Security will succeed in leading cyber security for the federal government and for critical infrastructure?

Almost all private sector victims conceal when their defenses have failed. Government agencies, in contrast, usually make incidents public. This disparity can distort our understanding of the problem. The failure to report most private sector breaches could give the impression that US-CERT's performance is below average, but when compared to private sector performance, US-CERT isn't doing badly. A better question is to ask is what networks aren't vulnerable to cyber attack (using the IG's terminology, which refers to incidents as 'attacks," although this is imprecise). In the last decade we have seen many Fortune 500 companies experience serious breaches, including major banks, defense contractors, large oil companies, chemical companies, auto companies, and many high-tech companies, along with many smaller firms,. Weak cybersecurity is a national problem.

In any case, US-CERT would not be administering the new authorities. The draft legislation is careful crafted to avoid a prescriptive, burdensome regulatory approach. It is modeled on standard business and accounting practices that leave it up to the individual firm to decide on the most effective way to comply with the law. Questions about DHS capabilities are a major and legitimate concern, but three points should be born in mind. First, in the last year DHS has begun to significantly improve its capabilities in the National Cyber Security Division. Congress should take up the oversight responsibility to require DHS to continue and accelerate these improvements. Second, DHS and DOD are developing a strong partnership that will let DHS draw upon DOD capabilities when needed. Third, the comparison with US-CERT no only begs the question as to whether the private sector is doing any better, it equates the risk of disrupting US-CERT with the risk of disrupting critical infrastructure. If US CERT was knocked off line for a week, there would be only minimal disruption; we may not feel the same way when it is our local power company that is hit.

Post-Hearing Questions for the Record
Submitted to Scott Charney
From Senator Tom Coburn

"Securing America's Future: The Cybersecurity Act of 2012"
February 16, 2012

1. From your perspective working for one of the leading technology firms in the world, can you please comment on the pace of technological change? Do cyber threats and hackers adjust to new security strategies and tactics quickly?

   Technology is evolving at an incredibly rapid pace. Its rapid evolution – and the introduction of new capabilities – has become a critical enabler of our information-based economy. Over the last ten years, we have witnessed the rise of the Internet citizen with members of society connected through email, instant messaging, video-calling, social networking, social searching, and a host of web-based and device centric applications. The surge in both cloud and mobile computing offer clear examples of the pace of technological change. New versions of software delivered as box products are typically available every few years. Yet, with the advent of cloud-based services and app-centric mobile devices, developers are able to deliver—and consumers are increasingly coming to expect—software innovations in a matter of months or even weeks.

   IT companies are not only innovating products and services, but also the processes and technology used to design, develop, deliver, and maintain the security of their offerings throughout their expected lifecycles. While efforts to improve the security of IT products and services have yielded significant improvements, those who seek to attack IT systems have also increased in both number and sophistication. According to the Special Edition of the Microsoft Security Intelligence Report released in February of this year,[1] approximately 60,000 forms of malware or threats were known to exist at the end of 2001. Today, estimates of the number of known computer threats such as viruses, worms, trojans, exploits, backdoors, password stealers, spyware, and other variations of potentially unwanted software range into the millions. Much of this malware is not designed to attack any particular organization; rather, it is opportunistic; it is unleashed with the hope that some random set of machines will be compromised. Additionally, we now also face threats from persistent and determined adversaries who will work, over time, to penetrate specifically targeted systems.

   In a world of such diverse threats, it is critically important that governments and cyber security professionals think differently about malicious cyber events and how to respond to them. This means embracing a two-pronged strategy.

   - First, those managing IT systems must improve their basic hygiene to counter opportunistic threats and make even persistent and determined adversaries work harder. This includes migrating to newer, more secure systems, or cloud services where security might be better managed; patching vulnerabilities promptly;

[1] http://www.microsoft.com/security/sir/story/default.aspx#!10year

configuring systems properly (in part through increased automation); educating users about the risks of social engineering; and taking other steps – whether they involve people, process, or technology – to manage risks more effectively than done today.

- The second part of the strategy involves dedicating specific resources and building expertise among computer security professionals to address the persistent and determined adversary. In many of these cases, the attacks are marked by long-term efforts to penetrate a computer system stealthily and then leverage the fact that a hard perimeter, once defeated, often reveals a soft interior that can be navigated easily for long periods of time with very little risk of detection. This being the case, the security strategy deployed for blunting opportunistic threats – a security strategy focused predominantly on prevention and secondarily on incident response – will not be enough. Instead, we must focus on four areas: prevention, detection, containment, and recovery.

While these elements are of course not new, there are opportunities to significantly increase our effectiveness in each. For example, while many organizations manage intrusion detection systems, security strategies have not focused on capturing, correlating and analyzing audit events from across the enterprise to detect anomalies that belie attacker movement. Additionally, recognizing how interconnected services have become, we need to focus on containment (e.g., network segmentation, limiting user access to least privilege) to ensure that, if part of a network is compromised, the adversary is well contained.

2. If a federal agency like the Department of Homeland Security issues cyber security standards and regulations, how quickly would hackers and our adversaries be able to adapt and exploit new vulnerabilities that the regulators are not prepared for or thinking about?

While hackers will work quickly to defeat security measures, eliminating risk should not be the goal of cyber security regulation. Put another way, sensible regulations would be designed to ensure have organizations have internal processes to manage risk better than is done today. At present, too many systems are not managed well; they are, for example, unpatched, misconfigured, or not monitored appropriately. As such, hackers can win, and far too easily. Therefore, establishing an appropriate security baseline, in collaboration with the private sector, is far better than accepting the current risk and will make it much more challenging for hackers to be successful. Over time, the baseline and standards will continue to rise, and at least United States enterprises, large and small, will be better positioned against hackers' evolving skills.

The ongoing battle between defenders and attackers and the innovations each uses is, in many ways, the crux of the challenge facing both government and industry in improving the security of critical infrastructures. Threats and technologies evolve dynamically and regulations typically cannot. Precisely for this reason, it is widely understood that government could never effectively improve the cyber security posture of our nation's

critical infrastructures by mandating adherence to a particular set of measures or compelling compliance with a specific list of regulatory requirements.

Microsoft has been engaging constructively with members and staff from both chambers and parties to address this challenge. It is my view that current legislative proposals from both the Senate and House could provide an appropriate framework to improve the security of government and critical infrastructure systems and establish an appropriate security baseline to address current threats. Furthermore, the frameworks are sufficiently flexible to permit future improvements to security – an important point since computer threats evolve over time.

To enable that flexibility for defenders, government should neither define specific standards nor controls. Rather government should work with industry to define security outcomes based on a strong understanding of threats and risks. Then industry, working with government, can develop internationally recognized, consensus-based standards to meet those defined outcomes. In such a model, government helps to set the bar, yet industry has flexibility to choose and, as necessary, modify specific controls, to address changing threats.

The key principles that we and many of our colleagues in industry have emphasized throughout the legislative process are as follows: Any effort to regulate the security of critical IT must be narrowly scoped to focus on those systems and assets that would cause catastrophic damage to national security, public safety, or economic stability. Governmental requirements for the security of those systems and assets should leverage existing standards, standard setting processes, and regulatory regimes. And companies that are acting in compliance with governmental requirements must be protected from frivolous litigation.