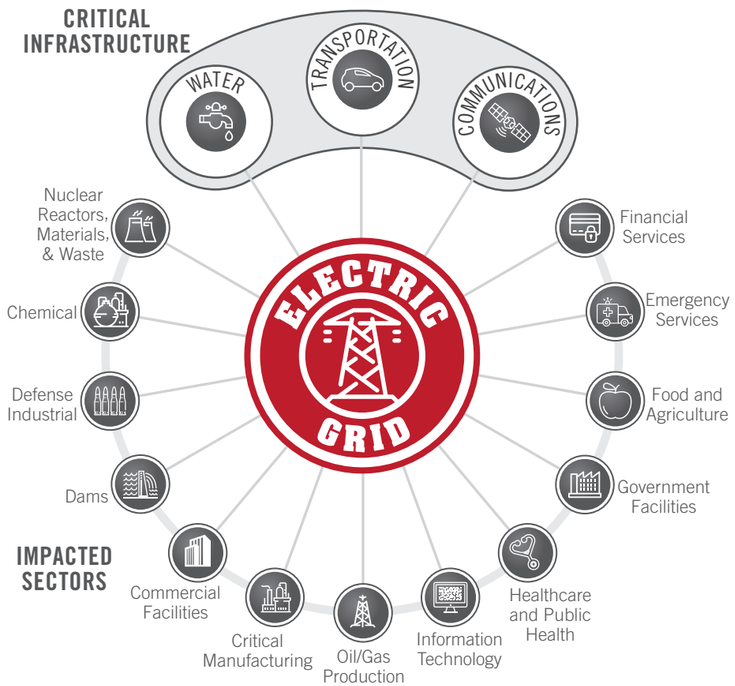
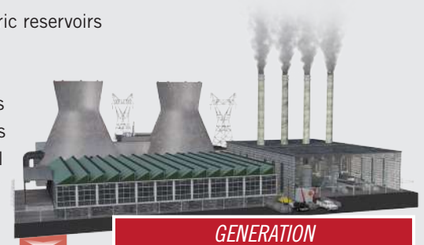
Complex Operating Environment—Electric Grid

The US energy sector consists of three interrelated segments: electricity, oil, and natural gas. The reliance of virtually all industries on electric power and fuels means that all sectors have some dependence on the energy sector. Information sharing is key to ensuring the protection of the national electrical infrastructure (electric grid) since the majority of it is privately owned. According to the US Energy Information Administration, the electric power sector contains more than 8,000 power plants with various owners and operators, including traditional electric utilities and private (non-utility) power producers. Approximately 30 percent of electricity produced occurs by combusting coal (primarily transported by rail), 20 percent by nuclear power plants, and 33 percent by combusting natural gas. The remaining generation is provided by hydroelectric plants (6 percent), oil (1 percent), and renewable sources (solar, wind, and geothermal) (3 percent).

Information sharing is critical as multiple jurisdictions oversee the electrical grid. As noted in DHS's 2015 Energy Sector-Specific Plan, energy serves as one of the four lifeline functions, along with water, transportation, and communications. A prolonged electrical outage will cause cascading effects to all other sectors. Emergency managers, owners and operators, and public safety personnel are encouraged to develop plans in advance, communicate priorities, and understand the effects of operating and maintaining services to each sector in the event of a mid- to long-term incident.



- Hydroelectric reservoirs
- Wind Farm
- Nuclear
- Fossil Fuels
- Natural Gas
- Geothermal
- Large solar farms



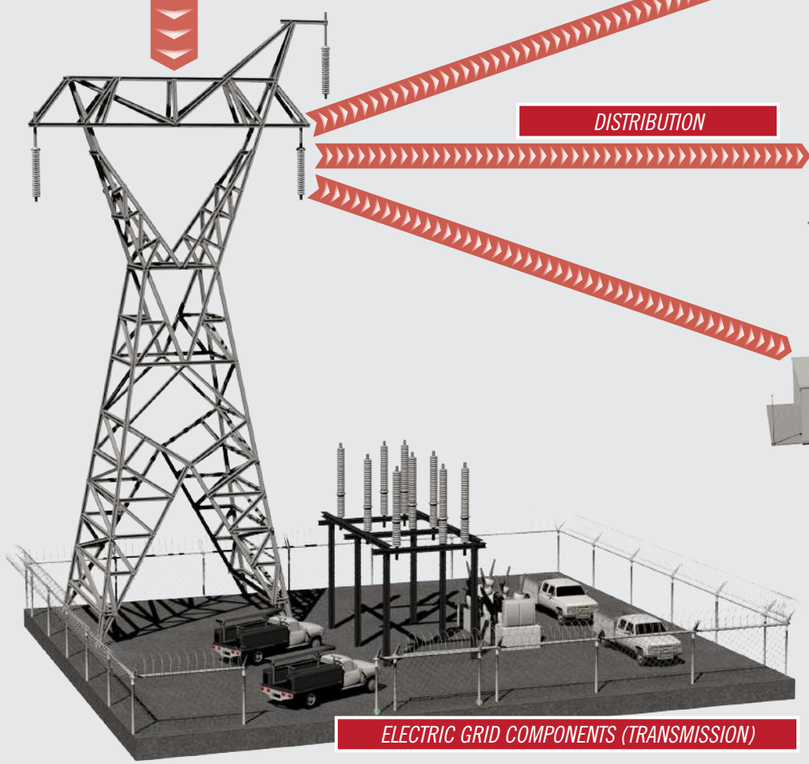
GENERATION

RESIDENTIAL

DISTRIBUTION

CITY/URBAN

INDUSTRIAL PLANT



ELECTRIC GRID COMPONENTS (TRANSMISSION)

- Substations
- Equipment, including transformers
- Transmission towers
- Battery storage

SECURING THE ELECTRIC GRID Virtually every community across the US has a power distribution infrastructure. While generation facilities may have on-site security resources, security at substations and maintenance equipment may depend on a number of factors. Transmission and distribution corridors typically remain unsecured. Many companies employ additional physical security protocols, including remote video surveillance, motion detection and alarm systems, but much of the grid's infrastructure is more accessible. Public safety personnel should become familiar with the locations of electric grid elements within their jurisdictions, including components that may be located within residential or business neighborhoods, such as substations, junction boxes, and battery storage sites. This will improve the ability of public safety personnel and owners and operators to identify and prioritize security of the most important components and protect themselves and the public in the unlikely event of an attack. This graphic highlights grid components and potential security concerns.

NCTC 031114 ID 5-18

REVISED 8 MAY 2018
AUTHORED BY NCTC, FBI, DHS

Complex Operating Environment—Electric Grid *(continued)*

We assess components of the electric grid may be potential targets of terrorists. Despite the limited number of terrorist attacks against the US electric grid, worldwide attacks against energy systems indicate ongoing interest by terrorists. Threats may emerge from a range of state and non-state actors with sufficient resources, who may be inspired by foreign terrorist organizations.

INDICATORS OF ATTACK While first responders, security personnel, and owners and operators may be in the best position to identify or recognize possible signs of a physical attack, owners and operators are most likely to detect a cyber incident.

Suspected attacks may require detailed physical examination and/or exploitation of the affected systems to determine an attacker's motive, delaying confirmation, and potentially impeding the timely implementation of protective measures. Natural and manmade hazards may also have an impact, requiring investigation to confirm the source of the disruption.

PHYSICAL ATTACKS have historically been done using low technology methods, including small arms fire, and sabotage. Indications of a physical attack or physical attack planning at electric grid nodes may include the following:

- Disruption of power service.
- Reports of explosions or suspected IEDs/VBIEDs.
- Visible active shooter or the sound of gunfire.
- Equipment fragments or physical damage to equipment.
- Fire or smoke.
- Suspicious vehicles.
- Unmanned aircraft systems activity or operators claiming they are flying for commercial purposes without appropriate documentation.
- Surveillance of the site or adjacent areas, including taking photographs or possessing maps or blueprints without a valid reason.
- Heavy equipment that does not belong at the site.
- Disruption of perimeter fencing or other physical security measures.

CYBER ATTACKS could use common computer intrusion techniques and open-source tools for network penetration and persistence. Similar to physical attacks, cyber threats could emanate from insider threats such as disgruntled employees or external threats, including state or non-state or lone actors.

Multiple coordinated or hybrid attacks consisting of physical and cyber elements may challenge power companies and law enforcement to determine the level of actors involved, their intent, or the extent to which attacks may be connected. Attacks on larger and more highly-connected substations or coordinated and/or simultaneous attacks on multiple smaller substations could cause substantial impacts for a large number of consumers.

FEDERAL RESPONSIBILITIES The primary Federal entities with roles related to security of the electric grid under normal and emergency conditions are the Department of Energy, the Department of Homeland Security, and the Federal Energy Regulatory Commission. Roles for these entities include standards and guidance, information sharing mechanisms, and the coordination of resource deployment during emergency events. However, in the event of a suspected terrorist attack, the FBI, in conjunction with other federal agencies, will operate as the lead investigatory agency.

PRE-INCIDENT CONSIDERATIONS First responders should be aware of accessible areas of the electric grid system and ways to work with government and private sector partners to improve communication and coordination, strengthen security, and improve the timing and efficiency of incident response.

REPORTING SUSPICIOUS BEHAVIOR Ensure reporting criteria, thresholds, and processes are established and used consistently to report suspicious behavior and activity. The Nationwide Suspicious Activity Reporting Initiative (NSI) provides education on Suspicious Activity Reporting (SAR) and SAR mechanisms. *https://nsi.ncirc.gov/*

INFORMATION SHARING Establish standard operating procedures for information sharing at all levels, including federal, state, local law enforcement, fusion centers, and the sector-based Information Sharing and Analysis Centers, as appropriate. *https://www.dhs.gov/homeland-security-information-network-hsin*

RESOURCES Maintain awareness of the various critical infrastructures within each agency's jurisdiction as well as in surrounding jurisdictions and know their main points of contact. In addition, have updated lists of available educational and training resources, such as the National Computer Forensics Institute. *https://www.ncfi.usss.gov/*

SAFETY Before an incident occurs, owners and operators and public safety personnel should work together to ensure that components of the electric grid are appropriately marked, outside and inside, to identify the specific hazards that may be present during an emergency response. For example, the National Fire Protection Association developed standardized markings aimed at first responders, which provides different information than the OSHA HazCom classification. *https://www.nfpa.org/Assets/files/AboutTheCodes/704/704_FAQs.pdf*

COMMUNICATION, COORDINATION, AND ENGAGEMENT Ensure utilities, public safety, and federal government liaisons communicate on a regular basis. Maintain relationships between the private and public sectors; engagement efforts could include developing definitions of suspicious behavior, training with utilities through tours and exercises, and developing a common terminology to describe threats and response capabilities. This will improve first responder knowledge of scene safety both prior to and after potential incidents and may include areas within facilities, which are inherently unsafe at all times. Joint training provides opportunities to develop mitigation plans when gaps are identified. *https://www.infragard.org/*

POST-INCIDENT CONSIDERATIONS Power interruptions may cause short- and long-term consequences for the power grid and the affected population. First responders and owners and operators are encouraged to communicate recovery priorities, which may not be the same for all incidents and may change during an extended power disruption. Generally, owners and operators will lead public messaging efforts. In coordination with the affected sectors and/or the industry's Electricity-Information Sharing and Analysis Center *(www.eisac.com)*, first responders and owners and operators should be prepared to communicate the following:

- Potential physical hazards at the scene that may affect remediation (scene safety). This could include obtaining official confirmation that all sources of electricity, including solar panels and batteries, have been turned off.
- Appropriate access and entry of first responder and utility personnel, including credentialing, if necessary.
- Potential crime scene considerations affecting evidence recovery or preservation.
- Guidance outlined in standard operating procedures and memorandums of understanding (MOUs), including notification requirements, jurisdictional concerns, and personnel safety criteria.
- Compliance with federal and state reporting requirements and other entities with investigative authority.
- Restoration protocols, including any additional critical facilities or equipment that may require protection.
- Expected lengths of power outages and potential affects to public safety capabilities.
- Plans to maintain life safety concerns (hospitals, emergency shelters) and restore public services and other community resources.
- Assistance required for securing and transporting replacement parts, components, or other equipment.

ELECTRIC GRID REPORTING REQUIREMENTS Many larger utilities have established incident-reporting requirements based on MOUs, permits, and contracts. However, smaller utilities may not have standard reporting procedures in place, resulting in less consistent notifications to law enforcement and fusion centers. First responders should work with owners and operators, relevant state regulators, and fusion centers to ensure mutual awareness regarding the reporting of suspicious activity, including:

- Benchmarks and suspicious reporting thresholds.
- Timeline and facts of the incident.
- Clear delineation of priorities of both private sector and law enforcement.
- The availability and presence of on-site equipment for use during or after an incident and equipment that may take time to replace.

ADDITIONAL ISSUES First responders are encouraged to work with owners and operators to understand and address the following potential issues:

- Cross-jurisdictional concerns, limitations on authorities or response capabilities, and the presence of other utilities within the same jurisdiction.
- Specific demographic and geographic characteristics of the distribution customers.
- Public messaging during and after an incident, including coordination and distribution, possibly across multiple platforms.
- Rules regarding physical control of the scene during and after an incident, including evidence recovery, mitigation of life safety hazards, and recovery operations.
- Remote surveillance/monitoring, which differs across the country, has implications for where, how, and for how long evidence of suspicious activity or attacks may be documented, stored and accessed.
- Environment and/or weather may affect electric grid components, possibly indicating a false attack or enabling terrorists to hide their suspicious activity or attacks.

ADDITIONAL INFORMATION For a review of the electric grid and its components, refer to the Department of Energy's infographic, "Understanding the Grid" and the DOE Electricity 101 and FAQ. *https://www.energy.gov/articles/infographic-understanding-grid*, *https://www.energy.gov/oe/information-center/educational-resources/electricity-101#sys3*

NCTC 031114 ID 5-18

REVISED 8 MAY 2018
AUTHORED BY NCTC, FBI, DHS

JOINT COUNTERTERRORISM ASSESSMENT TEAM | JCAT

PRODUCT FEEDBACK FORM

(U) JCAT MISSION: To improve information sharing and enhance public safety. In coordination with the FBI and DHS, collaborate with other members of the IC to research, produce, and disseminate counterterrorism (CT) intelligence products for federal, state, local, tribal and territorial government agencies and the private sector. Advocate for the CT intelligence requirements and needs of these partners throughout the IC.

NAME and/or ORG:

DISCIPLINE: ☐ LE ☐ FIRE ☐ EMS ☐ HEALTH ☐ ANALYSIS ☐ PRIVATE SECTOR DATE:

PRODUCT TITLE: NCTC-FBI-DHS (U) First Responders Toolbox - Complex Operating Environment - Electric

POOR  GREAT

ADDITIONAL COMMENTS, SUGGESTIONS, OR QUESTIONS. HOW DOES JCAT MAKE PRODUCTS BETTER?

WHAT TOPICS DO YOU RECOMMEND?

SUBMIT