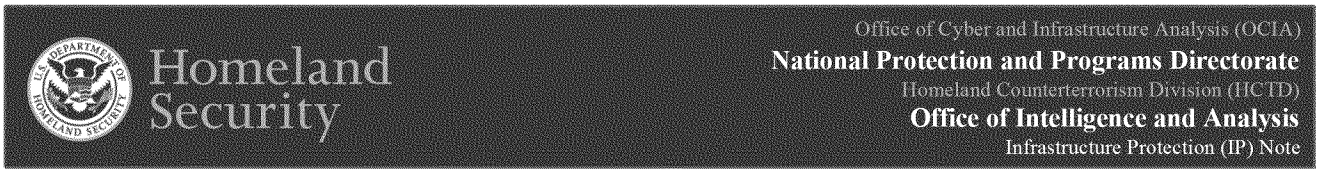


(U) IP Note: Most Significant Activity Surrounding Tactics, Techniques, and Procedures Against the Electricity Subsector

March 26, 2014, 1515 EDT

(U) SCOPE

(U) The Department of Homeland Security's Office of Cyber and Infrastructure Analysis (DHS/OCIA)[1] Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) produces Infrastructure Protection (IP) Notes to provide information on risks impacting the critical infrastructure community.

(U//FOUO) This IP Note is a joint publication of OCIA and the DHS Office of Intelligence and Analysis (I&A) Homeland Counterterrorism Division. It is intended to identify high-consequence tactics, techniques, and procedures (TTPs) used during attacks and incidents that occurred at electrical substations, facilities, and associated electrical infrastructure from 2002 to 2013. The incidents identified in this report have no known nexus to terrorism.

(U//FOUO) This IP Note utilizes information obtained from the Federal Bureau of Investigation (FBI), and has been coordinated with Department of Energy (DOE). Input was received from the National Protection and Programs Directorate's Federal Protective Service, and the Office of Infrastructure Protection's Sector Outreach and Programs Division, and the Protective Security Coordination Division. Information was also derived from open source reporting.

(U) KEY FINDINGS

- **(U//FOUO) Electricity subsector infrastructure components are vulnerable to many tactics. The most likely high-profile and potentially consequential TTPs are targeted shootings, intentional downing of power lines, and bombings.**
- **(U//FOUO) Targeted shootings at electrical substation critical infrastructure can cause extensive damage, but due to system resiliency, the effects may not result in significant impacts to customers.**
- **(U//FOUO) Intentional downing of power lines often result in immediate consequences in terms of short-term power outages.**

[1] (U) In February 2014, NPPD created the Office of Cyber and Infrastructure Analysis by integrating analytic resources from across NPPD including the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC) and the National Infrastructure Simulation and Analysis Center (NISAC).

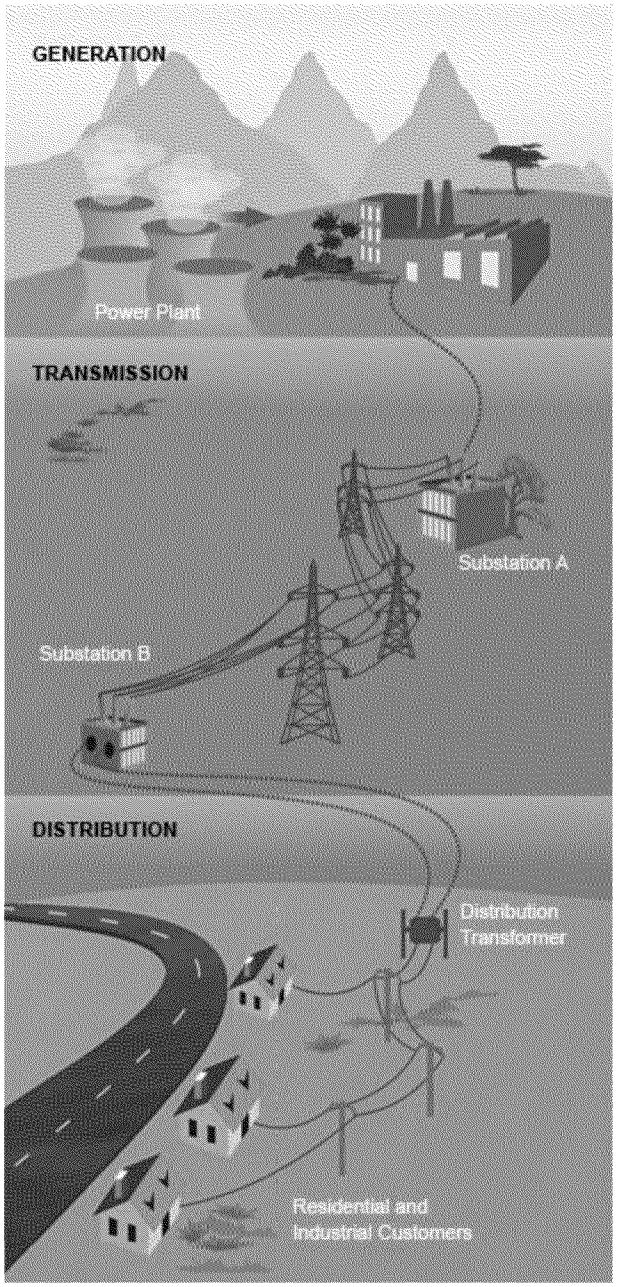
- **(U//FOUO) Bombings targeting substations have rarely been successful; however, a well-placed device can greatly reduce the capabilities of the substation.**
- **(U//FOUO) The financial impact from attacks against electricity subsector infrastructure can range from hundreds of thousands to millions of dollars in repair costs, even when power outages do not occur.**

(U) OVERVIEW

(U) Electricity subsector infrastructure includes electricity generation facilities, transmission substations, power lines, power pylons, control centers, and distribution substations.[2] Figure 1 illustrates these various infrastructure components.[3]

(U//FOUO) In the past decade, there have been thousands of intentional attacks and incidents in the United States against electricity subsector infrastructure. Targets have ranged from individual power lines to transmission substations and involved a variety of tactics. Effects from these incidents have varied, ranging from damaged components to power outages affecting thousands of customers.

(U) When suspicious incidents against electrical power infrastructure meet a certain threshold, owners and operators are required to file an OE-417 report with the DOE detailing the type, cause, and effect of the incident, as well as mitigating actions taken and any additional information (refer to the textbox on page 3 for more information on OE-417s and their analytic limitations). OCIA and I&A reviewed a sample of incidents reported to DOE between 2011and 2013, and open source data on events going back to 2002 to



(U) FIGURE 1.—Diagram of the Electric Power Generation, Transmission, and Distribution Process (Courtesy of CIMCON Software, Inc.)

[2] (U) DOE, "Energy Sector-Specific Plan," 2010, www.dhs.gov/xlibrary/assets/nipp-ssp-energy-2010.pdf.
[3] (U) For a more detailed discussion of the Electricity Subsector, see OCIA "(U) Infrastructure System Overview: The Bulk Power System," Washington, D.C.: U.S. Department of Homeland Security, September 23, 2013.

identify potential trends in TTPs and the intent or effects of these incidents.[4] Events categorized as suspected or actual physical attacks were the primary focus. The reported events ranged from damaged equipment, to theft of devices, and telephonic bomb threats against a facility. In addition to DOE-reported data, open source research focused on U.S. and North American incidents over the last decade.

(U) OE-417: Electric Emergency Incident and Disturbance Reports

(U) DOE's Office of Electricity Delivery and Energy Reliability uses OE-417 reports to monitor major system incidents on electric power systems. The criteria for submitting an OE-417 are listed below. If any of the first 8 criteria are met, a form must be submitted within1 hour of the incident. If any of the last 4 criteria are met, but none of the first 8, a report must be submitted within 6 hours.*

1. (U) Physical attack that causes major interruptions or impacts to critical infrastructure facilities or to operations.
2. (U) Cyber event that causes interruptions of electrical system operations.
3. (U) Complete operational failure or shutdown of the transmission and/or distribution electrical system.
4. (U) Electrical System Separation (Islanding) where part or parts of a power grid remain(s) operational in an otherwise blacked out area or within the partial failure of an integrated electrical system.
5. (U) Uncontrolled loss of 300 MW or more of firm system loads for more than 15 minutes from a single incident.
6. (U) Load shedding of 100 MW or more implemented under emergency operational policy.
7. (U) System-wide voltage reductions of 3 percent or more.
8. (U) Public appeal to reduce the use of electricity for purposes of maintaining the continuity of the electric power system.
9. (U) Physical attack that could potentially impact electric power system adequacy or reliability; or vandalism which targets components of any security systems.
10. (U) Cyber event that could potentially impact electric power system adequacy or reliability.
11. (U) Loss of electric service to more than 50,000 customers for 1 hour or more.
12. (U) Fuel supply emergencies that could impact electric power system adequacy or reliability.

(U) Analysis based on OE-417 event reports is subject to several important limitations. The report alerts DOE to electrical emergency incidents and disruptions. For events that occur on the bulk power system and do not meet the criteria of form OE-417, companies must submit a report to the North American Electric Reliability Corporation (NERC) under Reliability Standard EOP-004, Disturbance Reporting, within 24 hours of event occurrence. Companies may be required to submit incident reports on events that do not meet the threshold of an OE-417 or EOP-004 to relevant State authorities as required; however, this does not aid wide-area aggregation or analysis since an unknown percentage of events may not be incorporated into historical analysis. Also, whether or not an event is defined as an "attack" may vary due to how reporting entities choose to classify an event. In addition, those who fill out the forms are generally concerned with reporting operational or capacity issues and may not be aware of and include information of value from an intelligence or analytic perspective.

*(U) Office of Electricity Delivery and Energy Reliability, "OE-417 Electric Emergency Incident and Disturbance Report Instructions," Washington, DC: Department of Energy, January 2012, www.oe.netl.doe.gov/OE417/Content/OE-417_Instr-complete013115.pdf.

[4] (U) DOE; Pub Date: July 2013; DOI: Jan. 2011 – July 2013; Title: OE 417 Forms_2011-2013_Physical; Class: Unclassified; Src Desc: Excel spreadsheet, obtained by DHS/I&A from Department of Energy – derived from U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417.

(U) INFRASTRUCTURE IMPACT

(U//FOUO) Incidents against electrical power infrastructure have resulted in power outages of varying size and duration, and even when outages did not occur, impacts were felt in the cost to the power companies—and their customers—to fix damages. While no regional or national power outages resulted from any of the incidents reviewed, local disruptions have affected customers numbering from the tens to thousands or more. These outages have lasted from a few minutes to days, and repair and replacement costs can reach into the millions of dollars. For example, Entergy[USPER] officials estimate that a fire in 2013 at a switching station in Arkansas caused over $2 million in damages.[5]

(U//FOUO) Attacks against electric infrastructure have highlighted potential cascading vulnerabilities. The April 2013 Pacific Gas and Electric[USPER] (PG&E) Metcalf substation targeted shooting resulted in no outages, but if other substations that served the San Francisco region had also been targeted as part of a coordinated attack, it could have led to significant and persistent power outages.[6] Similarly, simulations conducted by OCIA (formerly HITRAC) after a July 2013 transmission line shooting in Arizona, determined that the loss of the affected line plus another transmission line in the vicinity could result in the remaining lines becoming overloaded.[7] In the October 2013 Cabot, Arkansas incident involving toppled electrical poles, a power company official testified that the loss of a transmission line could result in other lines overloading, jeopardizing the reliability of service, and potentially causing power outages in the area.[8]

(U//FOUO) Several incidents—including the April 2013 PG&E[USPER] Metcalf substation shooting, and October 2013 Cabot, Arkansas electrical pole toppling—have indications of insider information or in-depth knowledge of how and what to target to achieve maximum impact. This type of knowledge could be further used to impact electrical infrastructure in ways that could cause larger or longer outages or damage that is harder to repair. For example, extra high-voltage (EHV) transformers are the most vulnerable components in the electric grid. They are often located in remote substations, making them difficult to replace in an emergency. EHV transformers generally weigh hundreds of tons and are usually too large to transport by road, in some cases they must be moved with specialized rail cars. Across the nation there is a limited supply of EHV transformers because they are typically custom built and can take months or years to replace.[9] Multiple EHV transformers damaged at the same time can cause extensive economic effects.[10]

---

[5] (U) William Pentland, "FBI, Joint Terrorism Task Force Arrest Suspect In Arkansas Power Grid Attacks," *Forbes*, October 14, 2013, www.forbes.com/sites/williampentland/2013/10/14/fbi-joint-terrorism-task-force-arrest-suspect-in-arkansas-power-grid-attacks/.
[6] (U) OCIA, "(U) HSEC 8.8 – Energy | California Substation Shooting and Cable Cutting Incident – Update," 20 May 2013.
[7] (U) OCIA, "(U) Potential Impacts of the Loss of Transmission Lines in the Phoenix, Arizona Vicinity," 17 July 2012.
[8] (U) William Pentland, "Vandals Attack Electric Grid In Arkansas," *Forbes*, September 26, 2013, www.forbes.com/sites/williampentland/2013/09/26/terrorists-attack-electric-grid-in-arkansas/.
[9] (U) DHS, "Power Hungry: Prototyping Replacement EHV Transformers," Accessed October 21, 2013, www.dhs.gov/power-hungry-prototyping-replacement-ehv-transformers.
[10] (U) Office of Electricity Delivery and Energy Reliability, "Large Power Transformers and the U.S. Electric Grid," Washington, DC: Department of Energy, June 2012, http://energy.gov/sites/prod/files/Large%20Power%20Transformer%20Study%20-%20June%202012_0.pdf.

(U) Less serious incidents against electric power infrastructure generally have little to no discernible effect on power supplies or transmission. In the incidents of theft or vandalism reviewed, there was no loss of load and notification was typically made to nearby utilities to enhance investigation efforts and limit further disruption. In all reported cases, equipment was repaired, restored, and/or replaced in a timely manner with low interruption to power loads.[11]

(U//FOUO) Other reported incidents with infrastructure impacts included damaged transmission towers that caused the de-energizing of lines or transmission equipment. In those cases, reduced import limits and cancelled scheduled work reduced the risk of further equipment failure or damage.

(U) HIGH-CONSEQUENCE TTPS MOST COMMONLY USED

(U//FOUO) Three high-consequence TTPs are most commonly found in the available data; targeted shootings, intentional downing of power lines, and bombings. These TTPs are considered high consequence because they can create significant financial impacts to the subsector owner-operators, and costly power outages which impact customers. Within the data, these TTPs are categorized as vandalism, trespassing, and various other illegal acts. All of the reported events and their associated TTPs were considered criminal in nature.

(U) TARGETED SHOOTINGS

(U) Shootings at electric infrastructure have ranged from a single shot fired at a power line insulator to multiple coordinated shootings that impact an entire local system. Targeted shootings can be difficult to protect against given the stand-off distance from a target that firearms provide. In addition, the distance between the perpetrator and the targeted infrastructure may make it difficult to determine where the gunfire is coming from and may allow the perpetrator to escape unseen. Other vulnerabilities include the often remote and isolated locations of many electric power components. Most of these attacks are random acts of vandalism—particularly the shooting of insulators—rather than deliberate attacks on the sector, further complicating their characterization.

(U) There have been many incidents of gunfire targeting electric power components from 2011 to 2013. Notable incidents include the following:

- (U//FOUO) On 11 July 2013, a 500-kilovolt (kV) transmission line in the vicinity of Phoenix, Arizona, was damaged by rifle fire that targeted multiple insulation bells along the Navajo-Dugas line.[12] No outages resulted.

[11] (U) DOE; Pub Date: July 2013; DOI: Jan. 2011 – July 2013; Title: OE 417 Forms_2011-2013_Physical; Class: Unclassified; Src Desc: Excel spreadsheet, obtained by DHS/I&A from Department of Energy – derived from U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417.
[12] (U) OCIA, "(U) Potential Impacts of the Loss of Transmission Lines in the Phoenix, Arizona Vicinity," 17 July 3012.

- (U//FOUO) On 16 April 2013, the PG&E[USPER] Metcalf transmission substation in San Jose, California, was heavily damaged by gunfire targeting the radiators used to cool the transformers. Without functioning radiators to prevent overheating, the transformers were taken out of service. In a potentially related incident, just prior to the shooting, nearby underground fiber optic communication cables were severed in 2 separate locations, which disrupted 911 services in the area and affected some landline and cell phone service. However, no electrical outages resulted from the shooting.[13]
- (U) On 18 August 2011, a Greenville, North Carolina, Red Oak Community Rural Fire Department chief and an assistant chief were charged with shooting a 115-kV power line. Two insulators on a transmission line were shot, which severed the 115-kV line. The line fell to the ground and started a fire. The incident resulted in a 30-minute power outage affecting 16,000 customers.[14]
- (U) In December 2008, in Lebanon, Oregon, 4 campers shot at and destroyed 3 ceramic insulators attached to a large transmission tower that held several high-voltage power lines. The shooting downed a 115-kV electrical line. The damage resulted in an 80-minute power outage that affected thousands of customers.[15] The 4 men were sentenced to 5 years probation and ordered to pay the Bonneville Power Administration over $13,000 in restitution, by order of the Federal court that prosecuted the case.

(U//FOUO) The consequences of various shooting incidents differ depending on multiple factors, such as redundancies in the affected electric systems, intent of the incident, time of the incident, and the ability of the perpetrators to damage the most critical specific electric components. Based on historical data from open source and media reporting, more damaging attacks do not necessarily lead to power outages or other effects noticeable to consumers. For example, although the Metcalf shooting (referenced above) damaged 6 of 21 transformers and had the hallmarks of a perpetrator with insider or in-depth knowledge of that substation, PG&E[USPER] was able to continue operations with no loss of service.[16] It is likely, however, that if the incident had occurred during the day under peak loading conditions, instead of at night, the impact would have been more serious.

(U//FOUO) Protective measures remain consistent with guidance DHS/NPPD has provided in past documents. These measures include monitoring, surveillance, and inspection of property and equipment designed to protect electric transmission substations against threats and mitigate the effects of an attack. Installation of a closed-circuit television (CCTV) camera system, equipped with multiple color and black/white, fixed and Pan/Tilt/Zoom cameras, which provide 360 degree coverage of the site, is a standard practice for electric subsector infrastructure property. Further mitigation measures are installing alarms and intrusion detection devices, which will assist in monitoring activities of on-site contractors, vendors, and vehicles approaching the facility and could be leveraged for detecting preliminary threat indicators. Upon implementing surveillance detection equipment, owner/operators should regularly test alarms and intrusion

[13] (U) OCIA, "(U) HSEC 8.8 – Energy | California Substation Shooting and Cable Cutting Incident – Update," 20 May 2013.
[14] (U) Michael Abramowitz, "Firefighters Charged With Shooting Fixture," *The Daily Reflector*, August 18, 2011; www.reflector.com/news/firefighters-charged-shooting-public-power-fixture-621029, and http://statter911.com/2011/08/18/chief-assistant-chief-charged-with-shooting-power-line-down-fire-started-electricity-cut-for-16000-customer-in-red-oak-north-carolina/.
[15] (U) Associated Press, "Four Arrested For Shooting Down Major Power Line," *KATU2*, January 26, 2010, accessed October 17, 2013, www.katu.com/news/medicalalert/82706602.html.
[16] (U) OCIA, "(U) HSEC 8.8 – Energy | California Substation Shooting and Cable Cutting Incident – Update," 20 May 2013.

detection devices at facilities. These measures are unlikely to stop someone from shooting at a facility or power line component from longer range, but would at least increase the probability of apprehending the perpetrators, and could increase resiliency when used as a tool to identify damage to a site more rapidly.

(U) INTENTIONALLY DOWNING POWER LINES

(U) Power lines are an especially vulnerable component of the electric grid because there are hundreds of thousands of miles of transmission and distribution lines across the United States. Generally, power lines are easily accessible and have no particular protection, though they are also generally repairable within a short period of time. This may make them especially attractive targets to perpetrators who may have little or no specialized skills, but a desire to cause immediate, visible, though usually temporary, damage. Notable incidents include the following:

- (U) Between 21 August and 7 October 2013, there were three attacks on electrical infrastructure in and around Cabot, Arkansas. In the 21 August incident, the perpetrator downed a high-voltage transmission line.[17] In late September, the same person intentionally set a fire that destroyed a control house at a switching station, and on 6 October, he cut down two electric poles using a stolen tractor with a brush cutting attachment.[18] The first incident caused only a brief power outage that was quickly mitigated when the power company, Entergy[USPER], was able to reroute power to customers; the second incident did not result in any outages, but the damage from the fire alone was estimated at more than $2 million.[19,20] The third incident, however, resulted in a two-hour power outage to approximately 9,000 customers.[21] Authorities arrested the alleged perpetrator of all three incidents; his motive and any potential insider knowledge status or specialized skills are currently under investigation.
- (U) On 27August 2013, a local transit authority electrician driving a stolen 33-ton crane truck in Long Island, New York, used the truck's raised boom to pull down 15 utility poles, including two high-voltage transmission poles, as well as 12 transformers and 60 sections of primary and secondary wire. The damage knocked out power to more than 6,000 customers on Long Island.[22] The cost to repair all damages was estimated at more than $2 million and involved nearly 100 utility workers.[23] The perpetrator has alternately blamed his actions on a bipolar disorder and confusion caused by medications, and also claimed the incident was a joke.[24]

---

[17] (U) FBI, "FBI Offers Up to $20,000 Reward for Information Regarding Downed Cabot Power Line," August 22, 2013, www.fbi.gov/littlerock/press-releases/2013/fbi-offers-up-to-20-000-reward-for-information-regarding-downed-cabot-power-line.
[18] (U) William Pentland, "Weekend Attacks on Arkansas' Electric Grid Leave 10,000 Without Power; 'YOU SHOULD HAVE EXPECTED U.S.'," *Forbes*, October 7, 2013, www.forbes.com/sites/williampentland/2013/10/07/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/.
[19] (U) Jason Woodring, "Arrest Made Over Arkansas power Grid Attacks," *CBS News*, October 14, 2013, www.cbsnews.com/news/arrest-made-over-arkansas-power-grid-attacks/.
[20] (U) Ibid.
[21] (U) William Pentland, "Weekend Attacks on Arkansas' Electric Grid Leave 10,000 Without Power; 'YOU SHOULD HAVE EXPECTED U.S.'," Forbes, October 7, 2013, www.forbes.com/sites/williampentland/2013/10/07/weekend-attacks-on-arkansas-electric-grid-leave-10000-without-power-you-should-have-expected-u-s/.
[22] (U) Aisha Al-Muslim, Alfonso A. Castillo, Mark Harrington, John Valenti, and Patrick Whittle, "Cops: MTA Worker Joel Grasman Downed Poles, Wires In Elmont With Stolen Truck," *Long Island Newsday*, August 27, 2013, www.newsday.com/long-island/nassau/cops-mta-worker-joel-grasman-downed-poles-wires-in-elmont-with-stolen-truck-1.5963210.
[23] (U) Author unknown, "Transit Worker Joel Grasman Arraigned on Felony Charges in Elmont Outage Incident," *News 12 Long Island*, August 28, 2013, longisland.news12.com/news/transit-worker-joel-grasman-arraigned-on-felony-charges-in-elmont-outage-incident-1.5970783.
[24] (U) Ibid.

(U//FOUO) Consequences from attacks that down power lines often result in immediate local-area power outages and significant monetary damages. Downing the correct line (or lines) can instantly result in power outages to tens of thousands of customers. While the outages may be short lived, they can result in inconvenience to power consumers and large costs to electric utilities (which they may pass on to customers). Unlike other attack types targeting substations—such as shootings and bombings—system redundancies could be less effective when power lines are downed.

(U//FOUO) Owing to the accessibility of power lines, there are fewer effective protective measures than for other components of the electric power system. Crime prevention through environmental design (CPTED) is a multi-disciplinary approach/strategy that may offer some protection to power lines. CPTED assists in masking detectable vulnerabilities by installing shrubbery or trimming back bushes and tree limbs to an affected area to open the area up and allow ease of observation of the infrastructure or equipment. In some foreign countries with high threat to power lines, companies have built fences around individual power pylons, but this is very costly for companies and consumers. However, despite the difficulty in protecting power lines, they can generally be replaced or repaired quickly after an incident or attack.

(U) BOMBINGS

(U) Homemade bombs, also referred to as improvised explosive devices (IEDs), have generally been deployed against substations and pylons or lower voltage power poles. This TTP is often unsuccessful at transformer stations and other facilities because some degree of specialized knowledge in bomb construction and placement is required for maximum impact, and facilities are more likely to have security than remote power lines. Substations are complex facilities that house many types of equipment, often with redundant connections, so damage to part of a substation will not necessarily lead to the total loss of the substation or power outages for customers, depending on a substation's design or layout.[25] Bombs placed on power pylons can be effective because it can take several days or weeks to replace a high voltage tower that can be toppled with a relatively small explosive device due to the weight load and torque placed on towers by power lines.

(U) Examples of notable bombing, or attempted bombing incidents, targeting electric substations across the United States and Canada over the past decade include the following:

- (U) On 13 September 2013, in Red Deer, Alberta, Canada, a pipe bomb was found in a secured substation. Police removed and disposed of the bomb before it exploded. Authorities are speculating that it may have been the work of an insider or former employee because of the bomb's presence in a secure location.[26]
- (U) On 12 August 2010, in Lake St. Louis, Missouri, a pipe bomb exploded in the Woodland Marina electric substation, causing minor damage but no power outages. A chain link fence surrounding the property was cut. According to reporting, the substation may have been previously targeted; one year earlier, 4 gasoline-filled gallon jugs were

[25] (U) OCIA, "(U) Infrastructure System Overview: The Bulk Power System," Washington, D.C.: U.S. Department of Homeland Security, September 23, 2013.
[26] (U) Dave Dormer, "Mounties Respond Possible Bomb Found in Red Deer Secure Electrical Substation," *Calgary Sun*, September 13, 2013,www.calgarysun.com/2013/09/13/mounties-respond-possible-bomb-found-in-red-deer-secure-electrical-substation.

left on the property.[27] However, it is unknown whether the jugs were pre-positioned for subsequent malicious intent.

- (U) On 10 May 2005, a pipe bomb was found at an electric substation in Greensburg, Indiana. The device, which did not explode and was removed by police, appeared to have been thrown over the fence surrounding the substation. The incident was likely related to a similar one a month earlier at a nearby substation, and both were tentatively linked to a man charged with threatening to blow up the Indiana Statehouse.[28]
- (U) On 24 February 2002, on the last day of the Winter Olympics in Salt Lake City, Utah, a disgruntled Utah Power[USPER] employee detonated a homemade bomb between two breakers at an electric substation. The explosion knocked out power to 30,000 customers, the Salt Lake International Airport, and caused a fire at a nearby oil refinery.[29] The cost of the damage was estimated at approximately $217,000.[30]

(U) The consequences of electric power infrastructure bombings, especially substations, vary widely. The greatest concern arises from incidents in which bombs are placed by those with detailed or insider knowledge of substation equipment and operations, such as the 2002 Salt Lake City substation bombing, which affected 30,000 power customers.[31] However, most of the bombs in the analyzed incidents failed to explode as intended or were discovered and disposed of before they could explode. Successful bombings may result in expensive repairs for the utility (which may be passed on to customers) but do not necessarily cause power outages or damage to the power grid as a whole. Many types of equipment within substations are relatively easy to repair or replace, such as fuses. Even if parts of substation equipment are inoperable, other parts may be able to continue operating and work around the affected area. Total loss of a highvoltage transformer could take months or even years to replace depending on the presence of spares within the company, available inventory, or production line availability.

(U) Substation bombing consequences also depend on characteristics of the targeted substation, including its function, location, or current system design. For example, the loss of a transmission line along a critical path may have no impact on electricity consumers if designated contingency mitigation efforts exist and are properly implemented. An outage or disruption of a distribution substation, found in Figure 1, at the end of the network will affect a much smaller geographic footprint and account for a smaller number of customers affected.[32] Generally, bulk power systems are designed to withstand the loss of their single largest contingency, such as a generating unit or transmission facility on the system—known as *N*-1—and are sometimes

---

[27] (U) Joel Currier, "Suspected Pipe Bomb Explodes at Lake Saint Louis Electric Substation," *St. Louis Post-Dispatch*, August 13, 2010, www.stltoday.com/news/local/stcharles/suspected-pipe-bomb-explodes-at-lake-saint-louis-electric-substation/article_53a4211f-e254-5268-9ebc-8fcd59201e85.html.

[28] (U) Associated Press, "Bomb Found at Substation; Possible Link to Indiana Statehouse Threat," *SecurityInfoWatch*, May 11, 2005, www.securityinfowatch.com/news/10594600/bomb-found-at-substation-possible-link-to-indiana-statehouse-threat.

[29] (U) Angie Welling, "A Guilty Plea in Oly Bombing of Power Substation ," *Deseret Morning* News, August 7, 2003, www.deseretnews.com/article/1001724/A-guilty-plea-in-Oly-bombing-of-power-substation.html.

[30] (U) Author unknown, "Man Sentenced in Utah 2002 Olympics Power Explosion," *Firehouse Magazine*, October 16, 2003, www.firehouse.com/news/10528539/man-sentenced-in-utah-2002-olympics-power-explosion.

[31] (U) Angie Welling, "A Guilty Plea in Oly Bombing of Power Substation ," *Deseret Morning* News, August 7, 2003, www.deseretnews.com/article/1001724/A-guilty-plea-in-Oly-bombing-of-power-substation.html.

[32] (U) OCIA, "(U) Infrastructure System Overview: The Bulk Power System," Washington, D.C.: U.S. Department of Homeland Security, September 23, 2013.

designed so that the system can continue to function at *N*-2, operating reliably while missing two major elements.[33]

(U//FOUO) Planning and preparedness require coordinating all security-related activities to ensure protective measures are pertinent in mitigating bombing incidents. These measures include, but are not limited to, establishing a comprehensive security and emergency response plan; conducting regular liaison and communication activates with local and state law enforcement and emergency responders; and incorporating security awareness and response procedures into employee training programs. Specifically focused training programs concerning IEDs—including vehicle-borne IEDs—awareness/recognition and suspicious activity reporting procedures are integral to bombing incident mitigation. Further, conducting testing at regular intervals of an up-to-date emergency response plan and incident notification process, which cover all staff, is necessary for having an effective protective measures program.

(U) IMPACT FROM COOPER THEFT

(U) A number of the reviewed incidents involved the attempted or successful act of copper theft. The rising price of copper, combined with the ongoing economic crisis, has spurred perpetrators to steal copper grounding wires on utility poles, inside transformers and in substations, as well as copper wire from spools in unguarded or unlocked storage areas. Although we assess the majority of incidents involving copper theft is economically motivated, perpetrators can cause electrical blackouts as well as possible injury or death to utility company employees responsible for maintaining, servicing, and repairing damaged equipment.

(U//FOUO) OCIA assesses the *intent* of copper-theft is primarily for financial gains therefore, the *act* of cooper theft to electricity subsector infrastructure is not considered a TTP (in the context of this IP Note) for power supply disruption.

(U) Industry officials have taken some countermeasures to address the copper theft problem. These include the installment of physical and technological security measures, increased collaboration among the various industry sectors, and the development of law enforcement partnerships. Many states have also taken countermeasures by enacting or enhancing legislation regulating the scrap industry—to include increased recordkeeping and penalties for copper theft and noncompliant scrap dealers. However, there are limited resources available to enforce these laws, and a very small percentage of perpetrators are arrested and convicted. Additionally, as copper thefts are typically addressed as misdemeanors, convicted individuals pay relatively low fines and serve short prison terms.[34]

[33] (U) Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack, "Terrorism and the Electric Power Delivery System," Washington, DC: National Research Council of the National Academies, 2012, www.wiresgroup.com/docs/WPF_Terrorism%20and%20The%20Electric%20Power%20Delivery%20System.pdf.

[34] (U) Copper Theft Threatens U.S. Critical Infrastructure; www.fbi.gov/news/stories/2008/december/copper-theft-intel-report-unclass.

(U) Copper Theft

(U) Below are several examples of copper theft that led to outages:

- (U) On 30 September 2013, stolen copper grounding wire from an electrical substation at the University of California, Berkeley, caused a campus-wide power outage and also resulted in an explosion in an underground electrical vault.*
- (U) On 24 April 2013, stolen copper grounding wire resulted in a 2-hour power outage for 22,000 residents in Riverside County, California.†
- (U) On 6 January 2012, theft of copper wire from a substation in New Orleans, Louisiana disabled the entire substation, causing power outages that affected almost 4,000 customers.‡

(U) PG&E[USPER], which provides natural gas and electricity to 15 million people in northern and central California, estimates that it has experienced over 2,500 incidents of copper or metal theft resulting in a $5.5 million loss from 2005 to 2012.§ Incident reports filed with the DOE show that attempted and successful copper theft is a problem across the country and affects small and large utilities and jurisdictions. One way to mitigate the effects of copper theft over time is to replace copper—which is valuable and easy to melt down and sell—with other metals, such as aluminum or steel, that are less valuable. In Iraq a key component of stopping power line theft was switching from copper to aluminum cable.

---

* (U) Lyanne Melendez, "Officials: Stolen Copper Led to Cal Blackout," *ABC7 News,* October 1, 2013, abclocal.go.com/kgo/story?section=news/local/east_bay&id=9268785.

† (U) Tony Shin and Neil Costes, "Menifee Residents Furious Over Power Outage Caused by Copper Theft," *NBC Southern California*, April 26, 2013, www.nbclosangeles.com/news/local/Menifee-Residents-Furious-Over-Copper-Theft-Power-Outage-204778781.html.

‡ (U) Robert Morris, "Copper Theft at Entergy Substation Cuts Power to Thousands In Carrollton, University Areas," *Uptown Messenger*, January 6, 2012, uptownmessenger.com/2012/01/power-outage-affects-thousands-of-homes-in-carrollton-university-areas/.

§ (U) Author unknown, "Bay Area Power Outages Blamed On Copper Thieves, Downed Trees," *CBS San Francisco*, June 5, 2013, sanfrancisco.cbslocal.com/2013/06/05/bay-area-power-outages-blamed-on-copper-thieves-downed-trees/.

** (U) DOE; Pub Date: July 2013; DOI: Jan. 2011 – July 2013; Title: OE 417 Forms_2011-2013_Physical; Class: Unclassified; Sre Desc: Excel spreadsheet, obtained by DHS/I&A from Department of Energy – derived from U.S. Department of Energy Electricity Delivery and Energy Reliability Form OE-417.

(U) Report Suspicious Activity

(U) To report suspicious activity, law enforcement, Fire-EMS, private security personnel, and emergency managers should follow established protocols; all other personnel should call 911 or contact local law enforcement. Suspicious activity reports (SARs) will be forwarded to the appropriate fusion center and FBI Joint Terrorism Task Force for further action. For more information on the Nationwide SAR Initiative, visit http://nsi.ncirc.gov/resources.aspx.