



Current Information Bulletin & Request for Information

Suspicious Activity Regarding the Electrical Grid in New Jersey

February 27, 2014

(U//FOUO) NJ Regional Operations Intelligence Center (NJ ROIC) Intelligence & Analysis Threat Unit ~ ROIC201402-00417T

Summary

(U//FOUO) In the past year, the NJ Suspicious Activity Reporting System (NJ SARS) has received multiple reports of intrusions at electrical grid facilities in New Jersey. The NJ ROIC currently has no indication of any specific threats associated with these incidents, but provides this information for situational awareness and requests information on any similar, previously unreported incidents in New Jersey.

Context

(U//FOUO) The U.S. electric grid is a vast network connecting thousands of electricity generators to millions of consumers.¹ Across the United States, three incidents highlight the grid's vulnerabilities to potential threats:

- **January 2014:** In Tucson, Arizona, unknown subject(s) removed multiple bolts from an electric tower's support structure, increasing the potential for collapse and electrical service interruption. Several bolts were discarded in the immediate area; none of the material taken has significant recycle value. The deliberate manner of the bolt removal, including probable acquisition of the requisite tools, indicates sabotage rather than vandalism.²
- **October 2013:** In Jacksonville, Arkansas, an identified suspect allegedly conducted multiple acts of sabotage over several months. In August, the suspect apparently removed bolts from the base of a high-voltage transmission line tower and tried to bring down the 100-foot tower with a moving train. In September, the subject reportedly set a fire at a substation control house. In October, the subject cut into two electrical poles and used a tractor to pull them down, cutting power to thousands of customers.³
- **April 2013:** In San Jose, California, unknown subject(s) fired multiple shots at an electrical transmission substation, damaging several transformers. Authorities subsequently discovered intentionally cut fiber optic cables in a manhole. No motive or suspects have been identified.⁴ The Santa Clara County Sheriff's Office released a substation surveillance video showing bullets hitting the fence and causing sparks (pictured at right).⁵



¹ Massachusetts Institute of Technology, "The future of the Electric Grid," <http://web.mit.edu/mitei/research/studies/the-electric-grid-2011.shtml>, 2011

² FBI Newark Division, Activity Alert SIR-00000009627, "Sabotage to Electrical Power Stations, Towers, and Lines," 2/10/14

³ CNN, "Arkansas man charged in connection with power grid sabotage," www.cnn.com/2013/10/08/us/arkansas-grid-attacks, C. Carter, 10/12/13

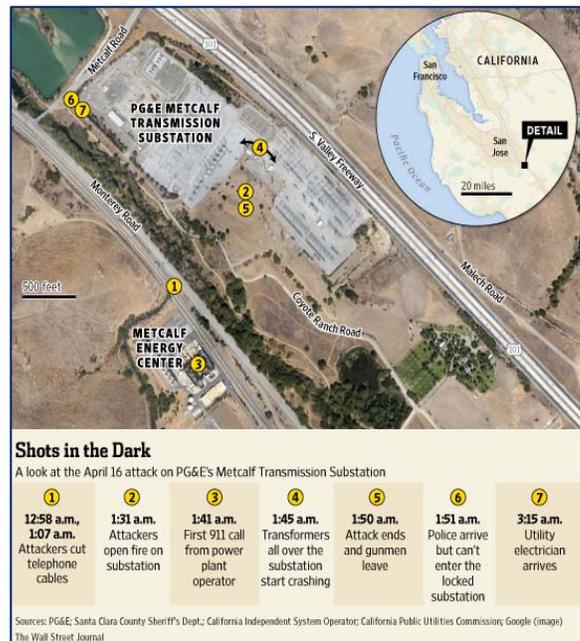
⁴ Northern California Regional Intelligence Center, Alert Bulletin, Incident Notification, "Vandalism to PG&E Substation Impacting Power and Telecommunications," 4/18/13

⁵ Santa Clara County California Sheriff's Office, PG&E Substation Surveillance Video, www.youtube.com/watch?v=RQzAbKdLw8, 6/4/13

(U) **INFORMATION NOTICE:** This product contains unclassified information that is for official use only (U//FOUO). Recipients should not release any portion of this product to the media, the public, or other personnel who do not have a valid need-to-know.

Tactics, Techniques & Procedures: San Jose Incident

(U) Media reports of the San Jose incident indicates that the unknown subject(s) entered an underground vault near the substation to cut fiber optic telecommunication cables. They were cut in a way that made them hard to repair and caused a phone blackout. It likely would have taken more than one person to lift the metal vault cover. The perpetrator(s) reportedly took a position 40 to 60 yards outside the substation fence, beyond the security camera's view. A surveillance camera recorded a streak of light - possibly a signal from a waved flashlight, followed by muzzle flashes and sparks from bullets hitting the fence. The shooter(s) apparently aimed at the transformers' oil-filled cooling systems. Riddled with bullet holes, the coolers leaked 52,000 gallons of oil, overheated, causing 17 transformers to crash. Another apparent flashlight signal, also caught on film, marked the end of the attack, which lasted less than an hour. Authorities found more than 100 shell casings from an assault rifle at the scene.^{6,7}



New Jersey Incidents

(U//FOUO) In the past twelve months, NJ SARS has received numerous reports of potential intrusions at electrical facilities in New Jersey, including:

- **January 26, 2014:** Employees found a hole, approximately three-foot high by two-foot wide, in the perimeter fence of an electric switching and substation in East Rutherford.⁸
- **January 22, 2014:** An identified subject entered a Burlington generating station using false identification. The subject claimed he had a gun (none found) and a bomb (package cleared).⁹
- **January 19, 2014:** Employees found a broken door at a Linden generating station. The steel door was pried open, causing a significant bend in the door, but nothing inside appeared to be disturbed.¹⁰
- **October 30, 2013:** Unknown subject(s) breached the main gate of a Burlington switching station and stole approximately 200 feet of commercial grade copper wire, valued at \$1,000.¹¹
- **October 14, 2013:** Unknown subject(s) cut the chain on the front gate of an electric switching and substation in East Rutherford.¹²
- **October 4, 2013:** An unidentified white male tried to enter a Cherry Hill substation by climbing the fence. When observed, the individual fled in a white Ford pickup truck. The subject has previously been seen taking items from a dumpster on the property.¹³

⁶ CNN, "Sniper attack on Silicon Valley power grid spurs security crusade by ex-regulator," www.cnn.com/2014/02/07/us/california-sniper-attack-power-substation/index.html, M. Martinez, 2/7/14

⁷ Wall Street Journal, "Assault on California Power Station Raises Alarm on Potential for Terrorism," <http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778>, R. Smith, 2/4/14

⁸ NJ Suspicious Activity Reporting System, CTLD10005350, 1/27/14

⁹ NJ Suspicious Activity Reporting System, CTLD10005322, 1/23/14

¹⁰ NJ Suspicious Activity Reporting System, CTLD10005328, 1/24/14

¹¹ NJ Suspicious Activity Reporting System, CTLD10005045, 11/4/13

¹² NJ Suspicious Activity Reporting System, CTLD10004960, 10/14/13

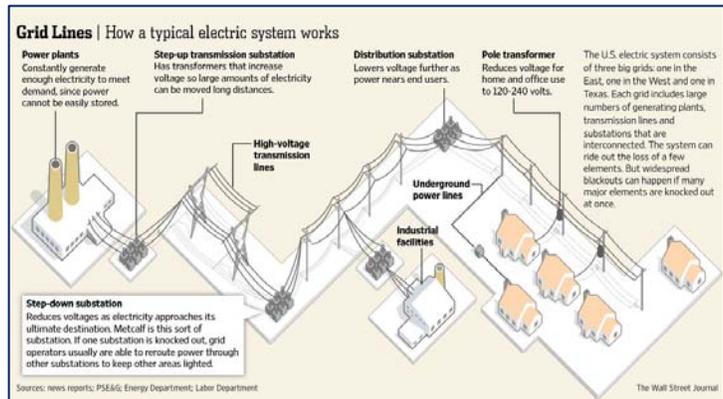
¹³ NJ Suspicious Activity Reporting System, CTLD10004924, 10/7/13

- **August 7, 2013:** A surveillance camera recorded an unidentified African American male (pictured at right), wearing gloves and carrying wire or bolt cutters at a Jersey City switching station.¹⁴
- **July 5, 2013:** A surveillance camera recorded two unidentified unauthorized African American males entering a Jersey City switching station.¹⁵



Assessment

(U//FOUO) The electrical grid - a network of power generating plants, transmission lines, substations, and distribution lines - is inherently vulnerable. Transmission substations are critical links in the electrical grid, making it possible for electricity to move long distances and serving as hubs for intersecting power lines. Many of the grid's important components sit out in the open, often in remote locations, protected by little more than cameras and chain-link fences.^{16,17}



(U//FOUO) The NJ ROIC currently does not have enough information to classify the New Jersey incidents listed above as indicative of pre-operational activity or connect them to a pattern. The incidents more likely involve vandalism and theft, rather than sabotage. However, any intrusion or damage to substations is a critical concern to the power supply and public safety.¹⁸

Potential Indicators

(U//FOUO) The following is a list of potential indicators of suspicious activity, including preoperational surveillance. A single indicator may not be suspicious by itself, but several indicators taken together may signify suspicious activity that warrants further investigation. Potential indicators include:

- Photographing objects or facilities that would not normally be photographed
- Individuals or vehicles loitering in sensitive areas with no valid reason
- Having maps or blueprints of a site with no valid reason
- Unusual or prolonged interest in security, entry points, access controls, or perimeter barriers
- Persistent questioning of facility personnel through personal contact, telephone, mail, or email
- Observing security drills, exercises, and reactions to possible threats, such as unattended packages
- Staring at and then averting gaze away from personnel or vehicles operating in secured areas, or displaying other anxious behaviors, such as retracing steps
- Monitoring radio scanners and recording emergency response times
- Mapping routes, timing traffic lights, and monitoring traffic flow in or near sensitive facilities
- Unexplained fire alarms or 911 calls, which may be attempts to observe emergency response
- Discreetly using cameras, binoculars, or note-taking and sketching at sensitive sites

¹⁴ NJ Suspicious Activity Reporting System, CTLD10004756, 8/21/13

¹⁵ NJ Suspicious Activity Reporting System, CTLD10004659, 7/24/13

¹⁶ Wall Street Journal, "Assault on California Power Station Raises Alarm on Potential for Terrorism," <http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778>, R. Smith, 2/4/14

¹⁷ DHS, Protective Security Coordination Division, Office of Infrastructure Protection, Infrastructure Report Series, Electrical Transmission Substations, 9/30/11

¹⁸ Northern California Regional Intelligence Center, Alert Bulletin/Incident Notification, "Vandalism to PG&E Substation Impacting Power and Telecommunications," 4/18/13

- Unfamiliar or out of place persons posing as panhandlers, protestors, vendors, news agents, etc.^{19,20}

(U//FOUO) Each indicator may be, by itself, lawful conduct and may constitute the exercise of rights guaranteed by the U.S. Constitution. There could be an innocent explanation for the behavior. For this reason, no single indicator should be the sole basis for law enforcement action. The totality of behavioral indicators and other relevant circumstances should be evaluated when considering any law enforcement response or action.

(U//FOUO) Facility personnel should remain vigilant and watch for observable behaviors, use field interrogation techniques to confirm or dispel reasonable suspicion, and document incidents through suspicious activity reports to the fusion center.

Potential Protective Measures

(U//FOUO) Potential protective measures against small-unit assault tactics, techniques, and procedures include:

- Use unpredictable security measures, including variable patrol times and routes, changing checkpoint locations and procedures, and periodically implementing additional measures
- Conduct joint scenario-based training and exercises that emphasize cooperation among first responders
- Conduct surveillance detection training and report suspicious activity
- Use internal surveillance systems accessible remotely by responding law enforcement²¹
- Identify high-value targets, increase security, and design a crisis reaction plan
- Conduct conspicuous training and response exercises in and around potential targets
- Use raised curbs, S-shaped entrances, and bollards outside a facility
- Be aware of traffic patterns and proximity of parked vehicles
- Use security cameras with opaque covers to conceal their operation
- Limit non-employee access to interior areas
- Establish controlled access points for delivery vehicles and limousine services
- Issue employee parking passes and employee identification that includes photographs^{22,23}

Request for Information

(U//FOUO) The NJ ROIC Intelligence & Analysis Threat Unit requests information on any similar, previously unreported incidents in New Jersey. Such suspicious activity should be reported immediately per existing agency protocols. Activity can also be reported 24 hours a day to the NJ ROIC Counter Terrorism Watch by phone, 866-4SAFENJ (866-472-3365) or 2-1-1, and email tips@njhomelandsecurity.gov.

Contact Information

(U//FOUO) Any agency with comments or questions about this document should contact the NJ ROIC at (609) 963-6900, ext. 6253, or njroicanalysis@gw.njsp.org.

¹⁹ FBI/DHS, Roll Call Release, "Terrorist Planning Cycle: Preoperational Surveillance," 7/9/10

²⁰ DHS, Protective Security Coordination Division, Office of Infrastructure Protection, Infrastructure Report Series, Electrical Transmission Substations, 9/30/11

²¹ FBI/DHS, Roll Call Release, "Update: Small-Unit Assault Tactics, Techniques, and Procedures," 7/5/11

²² FBI/DHS, Roll Call Release, "Terrorist Planning Cycle: Target Selection," 7/21/10

²³ DHS, Protective Security Coordination Division, Office of Infrastructure Protection, Infrastructure Report Series, Electrical Transmission Substations, 9/30/11