



(U//FOUO) Insider Threat to Utilities

19 July 2011

(U) Prepared by the Office of Intelligence and Analysis (I&A), Cyber, Infrastructure, and Science Division, Strategic Infrastructure Threat Branch and Cyber Threat Analysis Branch. Coordinated with the Control Systems Security Program, Industrial Control Systems–Computer Emergency Response Team; Environmental Protection Agency; and the Department of Energy.

(U) Scope

(U//FOUO) This Note is intended to support the activities of the Department and to assist federal, state, local, and tribal government counterterrorism and law enforcement officials and the private sector in preventing and responding to terrorist and criminal attacks against the critical public services provided by electric, gas, and water utilities in the United States. This note reviews recent incidents involving physical and cyber insider attacks and conveys the variety of threats posed by insiders to US utilities.

IA-0425-11

(U) Warning: This document is UNCLASSIFIED//FOR OFFICIAL USE ONLY (U//FOUO). It contains information that may be exempt from public release under the Freedom of Information Act (5 U.S.C. 552). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information and is not to be released to the public, the media, or other personnel who do not have a valid need to know without prior approval of an authorized DHS official. State and local homeland security officials may share this document with authorized critical infrastructure and key resource personnel and private sector security officials without further approval from DHS.

(U) All US person information has been minimized. Should you require the minimized US person information, please contact the I&A Production Branch at IA.PM@hq.dhs.gov, IA.PM@dhs.gov, or IA.PM@dhs.ic.gov.

(U) Key Findings

(U//FOUO) Disgruntled current and former utility-sector employees have successfully used their insider knowledge to damage facilities and disrupt site operations.

(U//FOUO) Outsiders have attempted to solicit utility-sector employees to obtain specific information about utility infrastructure site operations and facilities that could be useful in conducting physical and cyber attacks.

(U//FOUO) Because of their knowledge and authorized access to company information systems, insiders conducting cyber attacks have the potential to cause significant damage and disruption to utility facilities and operations.

(U) Source Summary Statement

(U//FOUO) Our judgments on the insider threat to utilities rely on open sources, law enforcement reporting, and US Government products. Based on the reliable reporting of previous incidents, we have high confidence in our judgment that insiders and their actions pose a significant threat to the infrastructure and information systems of US utilities. Past events and reporting also provide high confidence in our judgment that insider information on sites, infrastructure, networks, and personnel is valuable to our adversaries and may increase the impact of any attack on the utilities infrastructure.

(U//FOUO) Insider Threat

(U//FOUO) Disgruntled employees and adversaries seeking to use employees to obtain specific information about facility operations continue to pose a threat to utilities and other critical infrastructure. Current and former utility-sector employees often have detailed knowledge of site designs, layout, vulnerabilities, security protocols, and access procedures that could prove useful in planning attacks. Several recent incidents highlight the threat to infrastructure in the utility sectors from insiders and by outsiders seeking facility-specific information that might be exploited in an attack.

(U//FOUO) Physical Sabotage

(U//FOUO) Disgruntled current and former employees with insider access and expertise pose a potential physical threat to the utilities sector.

- (U) In April 2011, a lone water treatment plant employee allegedly manually shut down operating systems at a wastewater utility in Mesa, Arizona in an attempt to cause a sewage backup to damage equipment and create a buildup of methane gas. Automatic safety features prevented the methane buildup and alerted authorities, who apprehended the employee without incident.
- (U) In January 2011, a recently fired employee from a US natural gas company allegedly broke in to a monitoring station of his ex-employer and manually closed a valve, disrupting gas service to nearly 3,000 customers for an hour.

(U//FOUO) Cyber Attacks

(U//FOUO) Insiders often possess detailed operational and system-security knowledge, as well as authorized physical and systems access to utilities. Insiders can be employees, contractors, service providers, or anyone with legitimate access to utility systems. They often are self-motivated, know system security measures, and raise no alarms due to their authorized systems access. With knowledge of and access to a utility's network, malicious actors could seize control of utility systems or corrupt information sent to plant operators, causing damage to plant systems and equipment. Systems and networks used by utilities are potential targets for a variety of malicious cyber actors. Threat actors who target these systems may be intent on damaging equipment and facilities, disrupting services, stealing proprietary information, or other malicious activities. The greater the individual's knowledge and authorized systems access, the greater risk the individual poses. Furthermore, any individual with access to a plant's systems could unwittingly or inadvertently introduce malware into a system through portable media or by falling victim to socially engineered e-mails.

- (U//FOUO) In 2009, a disgruntled former information technology employee of a Texas power plant allegedly disrupted the company's energy-forecast system when the company failed to deactivate the employee's account access and confiscate his company-issued laptop after firing him weeks earlier. The cyber intrusion resulted in a \$25,000 loss to the company.
- (U) In 2006, a drinking water treatment plant in Harrisburg, Pennsylvania was compromised by a threat actor operating outside of the United States. Access was gained through a vulnerability in an employee's laptop, which allowed the installation of malware on the plant's internal system. The plant sustained no physical damage and the actual water system was not targeted in this particular incident. The objective was to use the plant's computer system to distribute e-mails.
- (U) In 2000, a contract employee, who became disgruntled after being turned down for a permanent position at an Australian wastewater services company, used his insider access and expertise to attack the facility's supervisory control and data acquisition (SCADA) systems. The attack disabled system functions and allowed a total of 800,000 liters of untreated sewage to spill into receiving waters over a period of several weeks.

(U//FOUO) Solicitation of Information

(U//FOUO) Outsiders have attempted to solicit employees to obtain specific information about utility infrastructure and site operations that could be useful in attacks. Solicitation efforts often involve outsiders falsely representing their identity and requesting access or information from facility insiders.

- (U//FOUO) In August 2010, a man was able to walk through the employee entrance of a North Carolina wastewater treatment plant administration building by posing as a member of the Army Corps of Engineers (ACE) going to Afghanistan. He claimed he was in the area preparing for a trip and inquired about the area the plant served. When he was informed that the facility was a

wastewater treatment plant and not a drinking water facility he stated that he was not interested and left. According to ACE, the unit with which the man claimed association is not an ACE organization.

(U) Violent Extremists with Insider Access

(U//FOUO) When violent extremists are able to gain access to an insider or acquire an insider position, this increases the likelihood of success and impact of an attack. Violent extremists have, in fact, obtained insider positions, and al-Qa'ida in the Arabian Peninsula (AQAP) has highlighted insider access as useful in attack planning.

- (U//FOUO) A US citizen who was arrested in Yemen in a March 2010 roundup of suspected al-Qa'ida members worked for several contractors performing non-sensitive maintenance at five different US nuclear power plants from 2002 to 2008. This individual was able to pass federal background checks, as recently as 2008, before becoming a contracted employee.
- (U//FOUO) The fall 2010 edition of AQAP's *Inspire* magazine encourages followers to conduct attacks using "specialized expertise and those who work in sensitive locations that would offer them unique opportunities" to conduct attacks.
- (U//FOUO) Senior al-Qa'ida officials have expressed interest in members acquiring positions that would provide access to sensitive or specialized information useful in attack planning.

(U//FOUO) Protective Measures

(U//FOUO) Alert facility personnel who report suspicious behavior and take appropriate precautions can help mitigate threats posed by insiders and the release of sensitive information. Other protective measures include:

- (U//FOUO) Obtaining and verifying work references, addresses, and phone numbers of all staff with access to controlled areas, including temporary, contract, and volunteer staff;
- (U//FOUO) Performing criminal background checks on all staff with access to controlled areas;
- (U//FOUO) Verifying the authorized access of all employees and visitors entering the facility;
- (U//FOUO) Defining controlled areas requiring security, limiting the number of access points, and securing all facility access points;
- (U//FOUO) Controlling access to remote and on-site information technology systems and logging and monitoring for inappropriate network activity;
- (U//FOUO) Conducting random security patrols of facility;

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) Maintaining secure backup information technology systems, and, where feasible, maintaining redundant backup systems, such as backing up the master terminal unit and SCADA systems;
- (U//FOUO) Providing regular security-related training to utility employees and emergency-response personnel;
- (U//FOUO) Cautioning employees not to discuss facility operations or related topics with outsiders;
- (U//FOUO) Requiring system users to sign a user agreement outlining proper use of facility systems and protection of sensitive facility data; and
- (U//FOUO) Ensuring systems access is deactivated immediately when an employee is no longer authorized access to facility systems.

(U) Outlook

(U//FOUO) We judge that terrorist groups and other adversaries will continue to seek employment opportunities and attempt to obtain information from insiders regarding utility infrastructure to improve attack planning and maximize damage. We judge that disgruntled and unstable employees in the utilities sectors will continue to pose a potential threat to the utilities sectors based on their access and intent. We judge that cyber attacks against utility-sector systems have the potential to cause significant damage and will continue to be a primary threat.

(U) Reporting Notice:

(U) DHS and the FBI encourage recipients of this document to report information concerning suspicious or criminal activity to the nearest State and Major Urban Area Fusion Center and to the local FBI Joint Terrorism Task Force. State and Major Urban Area Fusion Center contact information can be found online at <http://www.dhs.gov/contact-fusion-centers>. The FBI regional telephone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> and the DHS National Operations Center (NOC) can be reached by telephone at 202-282-9685 or by e-mail at NOC.Fusion@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the NOC. The NICC can be reached by telephone at 202-282-9201 or by e-mail at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

(U) I&A would like to invite you to participate in a brief customer feedback survey regarding this product. Your feedback is extremely important to our efforts to improve the quality and impact of our products on your mission. Please click below to access the form and then follow a few simple steps to complete and submit your response. Thank you.

(U) Tracked by: HSEC-1.4.2.9, HSEC-1.10.1, HSEC-6.1.2, HSEC-8.4.2, HSEC-8.6.2

CLASSIFICATION:



Homeland Security

Office of Intelligence and Analysis
I&A Customer Survey

Product Title:

1. Please select the partner type that best describes your organization.

2. Overall, how satisfied are you with the usefulness of this product?

- Very Satisfied**
 Somewhat Satisfied
 Neither Satisfied Nor Dissatisfied
 Somewhat Dissatisfied
 Very Dissatisfied

3. How did you use this product in support of your mission?

- Integrated into one of my own organization's finished information or intelligence products
- Shared contents with federal or DHS component partners
If so, which partners?
- Shared contents with state and local partners
If so, which partners?
- Shared contents with private sector partners
If so, which partners?
- Other (please specify)

4. Please rank this product's relevance to your mission. *(Please portion mark comments.)*

- Critical
- Very important
- Somewhat important
- Not important
- N/A

5. Please rate your satisfaction with each of the following:

	Very Satisfied	Somewhat Satisfied	Somewhat Dissatisfied	Very Dissatisfied	N/A
Timeliness of product or support	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Responsiveness to your intelligence needs	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

6. How could this product or service be improved to increase its value to your mission? *(Please portion mark comments.)*

To help us understand more about your organization so we can better tailor future products, please provide:

Name:	<input type="text"/>	Position:	<input type="text"/>
Organization:	<input type="text"/>	State:	<input type="text"/>
Contact Number:	<input type="text"/>	Email:	<input type="text"/>



[Privacy Act Statement](#)

[Paperwork Reduction Act Compliance Statement](#)

CLASSIFICATION: