



Information Bulletin

Title: Potential Vulnerabilities of U.S. Drinking Water and Wastewater Treatment Facilities to Insider Terrorism (U)

Date: August 11, 2004



Warning: This document is **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 or other personnel who do not have a valid “need-to-know” without prior approval of an authorized DHS official. This is a joint FBI and DHS Information Bulletin.

Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS national threat level is **YELLOW-ELEVATED**. The current threat level for the financial services sectors in New York City, Northern New Jersey and Washington, DC is **ORANGE-HIGH**.

DHS and FBI encourage recipients of this Information Bulletin to report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at <http://www.fbi.gov/contact/fo/fo.htm> – and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov. 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 (POC).

ATTENTION: State Homeland Security Advisors, State Drinking Water Administrators, State Public Health Agencies and their Laboratories, the Water Sector Information Sharing and Analysis Center (Water ISAC), Department of the Army Corps of Engineers, Department of the Interior, Federally-Operated Water Systems, Department of Health and Human Services and its Federal Public Health Agencies, and the Environmental Protection Agency.

OVERVIEW

(U//FOUO) Although DHS and FBI have no information that identifies a current credible threat to U.S. drinking water and wastewater treatment facilities, owners and operators should be aware of potential vulnerabilities to insider terrorist threats that could be both

UNCLASSIFIED//FOR OFFICIAL USE ONLY

physical and cyber in nature. This Information Bulletin looks at vulnerabilities that could be exploited by individuals who have access to water treatment process controls and treatment chemicals. It also identifies protective measures necessary to ensure the safety and integrity of the finished drinking water or wastewater systems.

(U//FOUO) While DHS and FBI possess no information indicating specific targeting of the U.S. drinking water and wastewater infrastructure, such targeting would be consistent with al-Qaida's stated objective to cause mass casualties and to disrupt and undermine vital economic interests in this country.

DETAILS

(U//FOUO) Information recently brought to the attention of DHS and FBI indicates that prior to the September 11, 2001 attacks; terrorists discussed possible attacks against U.S. facilities and systems to disrupt drinking water supplies serving major urban areas, which include large-capacity water reservoirs and water treatment facilities. Although no specific targets were selected, one specific site in the Northeastern United States was mentioned as an example.

(U//FOUO) While the original thought focused on large capacity water supplies, terrorists thought it would be futile to attempt to directly poison a large water reservoir because of the dilution factor. Rather, they focused on the possibility of poisoning the water during the water treatment process. Terrorists mentioned inserting a poison (not further identified) into the chlorination section of the water treatment facility. To accomplish this objective, they discussed recruiting insiders to work with them. DHS and FBI have no evidence that any operatives were dispatched to the United States after 9/11 to further plan or carry out such attacks. Nevertheless, DHS believes this information should be viewed as one of many legacy plots that could be revisited by terrorists.

(U//FOUO) DHS and FBI further assess that information discussed by the terrorists exhibits a certain degree of operational sophistication and is of particular concern for largely unattended drinking water or wastewater treatment facilities.

SUGGESTED PROTECTIVE MEASURES

(U//FOUO) The potential threat could derive from an insider's intentional introduction of a hazardous chemical into the treatment process through one or more of the chemical feed points within the treatment facility, or potential alterations to flow-paced chemical injection equipment. An outsider could achieve the same terrorist objective through intentional delivery or substitution of the wrong treatment chemical. The latter would necessarily involve some knowledge of the treatment processes and chemicals used inside the treatment facility; therefore, protective measures described below cover both scenarios.

Insider Threat through Introduction of Hazardous Chemicals into the Treatment Process

Consider the following protective measures:

- (U//FOUO) Perform a thorough check of the credentials provided by current and new employees (i.e., insiders) to ascertain any possible terrorist connections. If in doubt, check with the local FBI Office. A document providing guidance on establishing security policies, *Security Practices Primer for Water Utilities*, is available from the American Water Works Research Foundation (AWWRF) or is available to Water ISAC subscribers at www.waterisac.org.
- (U//FOUO) Ensure that suspected disgruntled employees or former employees do not have unescorted or unsupervised access to chemical injection or addition points within the treatment facility or at wells.
- (U//FOUO) Pay particular attention to contractors and vendors. Do not allow unescorted access to critical areas of the treatment facility by any contractor or vendor.
- (U//FOUO) Verify that access to remote chemical addition points is secured.
- (U//FOUO) Ensure that chemical injection points or chemical addition areas within the treatment facility are closely monitored. If possible secure these areas and promote the “buddy system.” Do not allow unauthorized personnel access to these critical areas.
- (U//FOUO) Validate the SCADA system, if used for flow-paced chemical feeds, has alarm functions for overfeeding.
- (U//FOUO) Ensure that the SCADA terminals and systems, if used, are only accessible by authorized personnel. Consider deploying strong user authentication methods such as one-time passwords, smart cards, biometric IDs, etc.
- (U//FOUO) Ensure compliance with best practice Cyber Security Standards such as those issued in June 2002 by the North American Electric Reliability Council (NERC) at: <http://www.esisac.com/library-guidelines.htm> . If SCADA system is accessible from the Internet or via remote dial-up review your intrusion detection and prevention solutions.
- (U//FOUO) Confirm that the SCADA system is running on a secure platform that will not allow unauthorized changes or access to the system files or control applications.

UNCLASSIFIED//FOR OFFICIAL USE ONLY

- (U//FOUO) Ensure that field-deployed remote terminal units (RTUs) and programmable logic controllers (PLCs) are in tamper proof enclosures. Conduct frequent loop back checks of the system for integrity. Do not allow unauthorized access to PLCs or RTUs.
- (U//FOUO) Consider using test kits and deploying advanced chemical and biological sensors to sample finished water in the clear well, or, in the case of groundwater direct pumping, at the entrance to the distribution system. For examples of available test kits/sensors see the Association of Analytical Communities (AOAC) website <http://www.aocac.org/testkits/TKDATA2.HTM>. A preliminary list of test kit components for water utilities is posted on the Water ISAC web page and is available to subscribers at www.waterisac.org. For additional information on field-ready monitors please see the following web site <http://www.epa.gov/etv/>.

Outsider Threat through Delivery of the Wrong Chemical

Consider the following protective measures:

- (U//FOUO) Do not allow unauthorized access to your facilities.
- (U//FOUO) Certify that the facility has a chemical delivery integrity program and “know your suppliers and vendors.” At a minimum, ensure that the chemical manufacturer has a Quality Assurance/Quality Control (QA/QC) program. If the delivery carrier is different from the manufacturer, also ensure the carrier has a QA/QC program.
- (U//FOUO) Ensure that the chemicals delivered are indeed the chemicals that were ordered. Check all chemical deliveries for driver identification and verification of cargo and ensure that the tankers, containers or cylinders have not been tampered with.
- (U//FOUO) Immediately report any suspicious or surveillance-type activities around treatment facilities to the local JTTF Office.

For comments or questions related to the content or dissemination of this Information Bulletin, please contact the DHS/Information Analysis and Infrastructure Protection Directorate’s Requirements Division at DHS.IAIP@DHS.GOV.