



WaterISAC

Water Security Network

www.WaterISAC.org



WaterISAC

What is WaterISAC?

- ✓ ISAC = Information Sharing & Analysis Center
- ✓ WaterISAC was formally launched soon after the 9/11 attacks.
- ✓ Developed by utility managers specifically for water sector utilities and state water agencies ... at the urging of U.S. EPA and the FBI's National Infrastructure Protection Center.



WaterISAC

More about WaterISAC

- ✓ Overseen by a board comprised of utility managers appointed by AWWA, AMWA, WEF, NACWA, NRWA, NAWC, ASDWA, AwwaRF and WERF.
- ✓ Designated by the Water Sector Coordinating Council as the water sector's official information-sharing arm. (The WSCC is a federal advisory panel to DHS comprised of utility managers.)
- ✓ Federal cost-share support has been provided by Congress through a grant from U.S. EPA.



WaterISAC

WaterISAC's Mission

- ✓ WaterISAC provides utility managers and state water agency directors with intelligence analysis, threat alerts, direct access to contaminant databases and more than 2,500 documents on security and emergency preparedness.
- ✓ WaterISAC is the ONLY national resource for sharing vital information on homeland security threats and other hazards.



WaterISAC

Why WaterISAC?

- ✓ Security incidents
- ✓ Weather emergencies
- ✓ Infrastructure losses



WaterISAC

WaterISAC: Two Options

WATERISAC
PRO

WATERISAC
BASIC



WaterISAC

WaterISAC BASIC VS. WaterISAC PRO SERVICES

FEATURE	DESCRIPTION	BASIC	PRO
24/7 Rapid Notification of National Water-Related Alerts and Advisories	Information from EPA and other federal agencies is sent via email. These important and helpful email alerts are free. To register visit www.WaterISAC.org .	X	X
	<p>Highly sensitive information, which the WaterISAC security team analyzes prior to dissemination.</p> <ul style="list-style-type: none"> • Includes region-specific notifications. • Includes infrastructure advisories. • Critically urgent information is sent via email, phone and PDA. 		X
Notification of Cyber Vulnerabilities	Cyber vulnerabilities intended for general public viewing.	X	X
	Cyber vulnerabilities containing highly sensitive information.		X
Secure Internet Portal	The secure Internet portal works like a website, however it contains an extremely secure means of access and authenticating its users. All <i>highly sensitive</i> information is disseminated via the secure portal . Pro subscribers are issued an authentication device, which authorizes access to the secure portal .		X
Quick Incident Reporting	WaterISAC receives information from utilities throughout the U.S. and Canada, which is compiled, sorted and analyzed by our team of water security experts. Pro subscribers may report incidents via the secure portal .	X	X
Online Database of Contaminants	The WaterISAC secure portal contains a vast database of contaminants and appropriate protocols that is quickly accessible and searchable. Contaminants include biological, chemical, radiological and nuclear agents.		X
Direct Access to Security Documents, Reports, Advisories, Bulletins and Updates	Information is stored and archived on the WaterISAC secure Internet portal and may be accessed anytime by the Pro subscriber. Information is quickly and easily searchable and provides invaluable information specific to the water sector.		X
24/7 Access to the Operations Center	A member of our WaterISAC security team is available by email or phone, 24 hours a day, 7 days a week.		X
Security Incident Reports with Analysis and Trends	WaterISAC collects incident reports and distributes a brief summary each month and a comprehensive assessment each quarter.		X
Emergency Preparedness, Response Plan, and Vulnerability Assessment Tools and Resources	WaterISAC and its team of water security experts have clearly defined procedures and protocols and will help you devise effective emergency preparedness and response plans for your utility. We will also assess your vulnerabilities and advise on appropriate actions.		X



WaterISAC

WaterISAC Pro Subscriptions

Annual subscription fees are modest:

- ✓ Fees are nominal compared to the value members receive with a WaterISAC Pro subscription
- ✓ Fees for utilities are based on utility size and service population

Service Population	Annual Fee for Primary User	Annual Fee for Each Add'l User
More than 100,000	\$1,000	\$500
50,000 to 100,000	\$500	\$250
Less than 50,000	\$200	\$100



WaterISAC

WaterISAC Pro: One of a Kind

- ✓ Has a 24/7 team of intelligence analysts, who have federal TOP SECRET clearances.
- ✓ Delivers threat information by email and text messaging.
- ✓ Hosts a secure forum for collaboration.
- ✓ Helps subscribers demonstrate due diligence.
- ✓ Exempt from the Freedom of Information Act.
- ✓ Protects sensitive information with signed non-disclosure agreements.

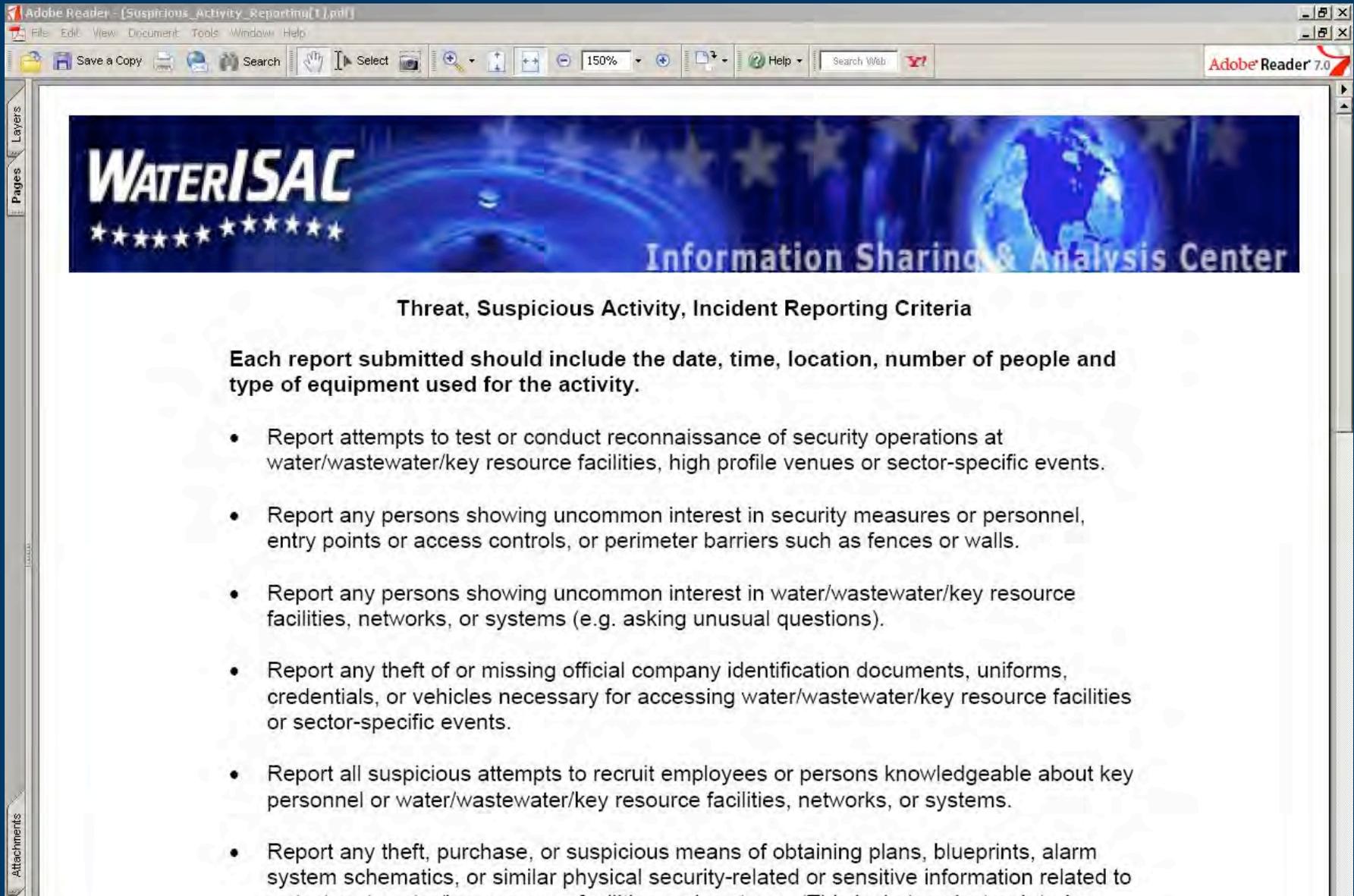


WaterISAC

Intel and Information Partners

- ✓ Central Intelligence Agency
- ✓ Department of Homeland Security
- ✓ FBI
- ✓ Department of Defense
- ✓ State Fusion Centers
- ✓ Homeland Security Agencies
- ✓ AwwaRF
- ✓ Private and proprietary information sources

Help in Identifying Suspicious Activity



WATERISAC

Information Sharing & Analysis Center

Threat, Suspicious Activity, Incident Reporting Criteria

Each report submitted should include the date, time, location, number of people and type of equipment used for the activity.

- Report attempts to test or conduct reconnaissance of security operations at water/wastewater/key resource facilities, high profile venues or sector-specific events.
- Report any persons showing uncommon interest in security measures or personnel, entry points or access controls, or perimeter barriers such as fences or walls.
- Report any persons showing uncommon interest in water/wastewater/key resource facilities, networks, or systems (e.g. asking unusual questions).
- Report any theft of or missing official company identification documents, uniforms, credentials, or vehicles necessary for accessing water/wastewater/key resource facilities or sector-specific events.
- Report all suspicious attempts to recruit employees or persons knowledgeable about key personnel or water/wastewater/key resource facilities, networks, or systems.
- Report any theft, purchase, or suspicious means of obtaining plans, blueprints, alarm system schematics, or similar physical security-related or sensitive information related to water/wastewater/key resource facilities and systems. (This includes electronic/physical

Incident, Suspicious Activity Reporting

Water Suspicious Activity Reporting Form - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Recycle Bin Mail Print W Yellow Speech M People

Address <https://subscribers2.waterisac.org/amwa/incident/incidentReport.asp> Go

Threat, Suspicious Activity, and Incident Report Form

When in Doubt, Report!

Please use this WaterISAC form to report threats, suspicious activity, and incidents to critical infrastructure.

Information concerning the identity of the reporting agency, department, company, or individual(s) will be treated on a confidential basis.

Contact Data for Person Filing Report (This can be left blank for anonymity)

Name

Telephone

Originator's Email

A WaterISAC Analyst will contact you once the information has been received.

Threat, Suspicious Activity and Incident Reporting

Instructions: Please provide as much information as possible. If you have any questions about a particular entry, please contact a WaterISAC analyst at 1-866-426-4722 option 4.

Date and Time of Event

Date/Time June 15 2007 08 : 37



WaterISAC

WaterISAC's National Incident Database

- ✓ Created by WaterISAC with information from law enforcement, open source, federal agencies and water utilities.
- ✓ With the data collected, WaterISAC analysts produce monthly incident summaries and quarterly trend analyses for subscribers.



WaterISAC

Security Incidents in 2007

- ✓ Pipe bombs found in a California water aqueduct.
- ✓ A subject broke into a water plant, cut the power and attempted to disable the SCADA system.
- ✓ A break-in at a water facility resulting in a control panel being manipulated and all the switches moved to open the valves leading to a backflow.
- ✓ An unidentified subject at a Maryland watershed impersonated a police officer and demanded access to a utility perimeter gate.



WaterISAC

1st Quarter Trends for 2008

- ✓ No change in number of inquires by persons trying to obtain sensitive facility information.
- ✓ Increase in break-ins/vandalism/theft that involve critical infrastructures.
- ✓ Decrease in contamination attempts.
- ✓ Increase in cyber-related threats and incidents.



WaterISAC

WaterISAC Threat Estimate / Q1

- ✓ Attacks using chlorine enhanced IEDs & VBIEDs have decreased in Iraq.
- ✓ Thefts of chemicals from water and wastewater facilities in the U.S. are most likely due to criminal behavior associated with the production of methamphetamine. Although anhydrous ammonia is the chemical needed for methamphetamine production, gaseous chlorine is often mistakenly stolen.
- ✓ Increased security measures at water and wastewater facilities in the U.S. have reduced the likelihood of the theft of gaseous chlorine.
- ✓ Should terrorists attempt to contaminate drinking water, they would most likely attempt to contaminate the finished water supply through the distribution system possibly using backflow. According to federal sources, many threats to contaminate water using backflow techniques were received in the 2006-2007 timeframe.



WaterISAC

Monthly Cyber Attack Trends



WaterISAC

Cyber

Attack Protocol/Port Summary - EWA-Canada/CanCERT™ Networks

Country	Current Period February 1, 2008 to February 29, 2008		Previous Period January 1, 2008 to January 30, 2008		Summary Period December 1, 2007 to Feb 29, 2008	
	Rank	% of Incidents	Rank	% of Incidents	Rank	% of Incidents
United States	1	33.23%	1	32.83%	1	32.87%
China	2	15.70%	2	13.64%	2	15.41%

Protocol Port Number	Service	Current Period February 1, 2008 to February 29, 2008		Previous Period January 1, 2008 to January 31, 2008		Summary Period September 1, 2007 to January 31, 2008	
		Rank	% of Incidents	Rank	% of Incidents	Rank	% of Incidents
UDP 1026	Unassigned	1	6.0	1	2.5	1	12.7
UDP 1027	Unassigned	2	5.9	2	2.2	2	9.5
UDP 1028	Unassigned	3	5.9	3	2.2	3	9.5
TCP 139	NETBIOS Session Service	4	0.8	4	0.3	5	1.9
TCP 445	Microsoft-DS	5	0.8	5	0.3	4	1.9
TCP 135	Location Service	6	0.7	6	0.2	6	0.8
TCP 5900	Unassigned	7	0.6	11	0.1	11	0.4
UDP 137	NETBIOS Name Service	8	0.4	7	0.2	7	0.8
UDP 1434	Microsoft-SQL- Monitor	9	0.3	8	0.1	8	0.7
TCP 1433	Microsoft-SQL-Server	10	0.2	9	0.1	9	0.5

.06%
.97%
.65%
.61%
.50%
.43%
.13%
.11%

Attack
the total

The above table provides a comparison of the EWA-Canada/CanCERT™ sensor top 10 ports and protocols along with a comparison to the previous month and the total for the previous six months.

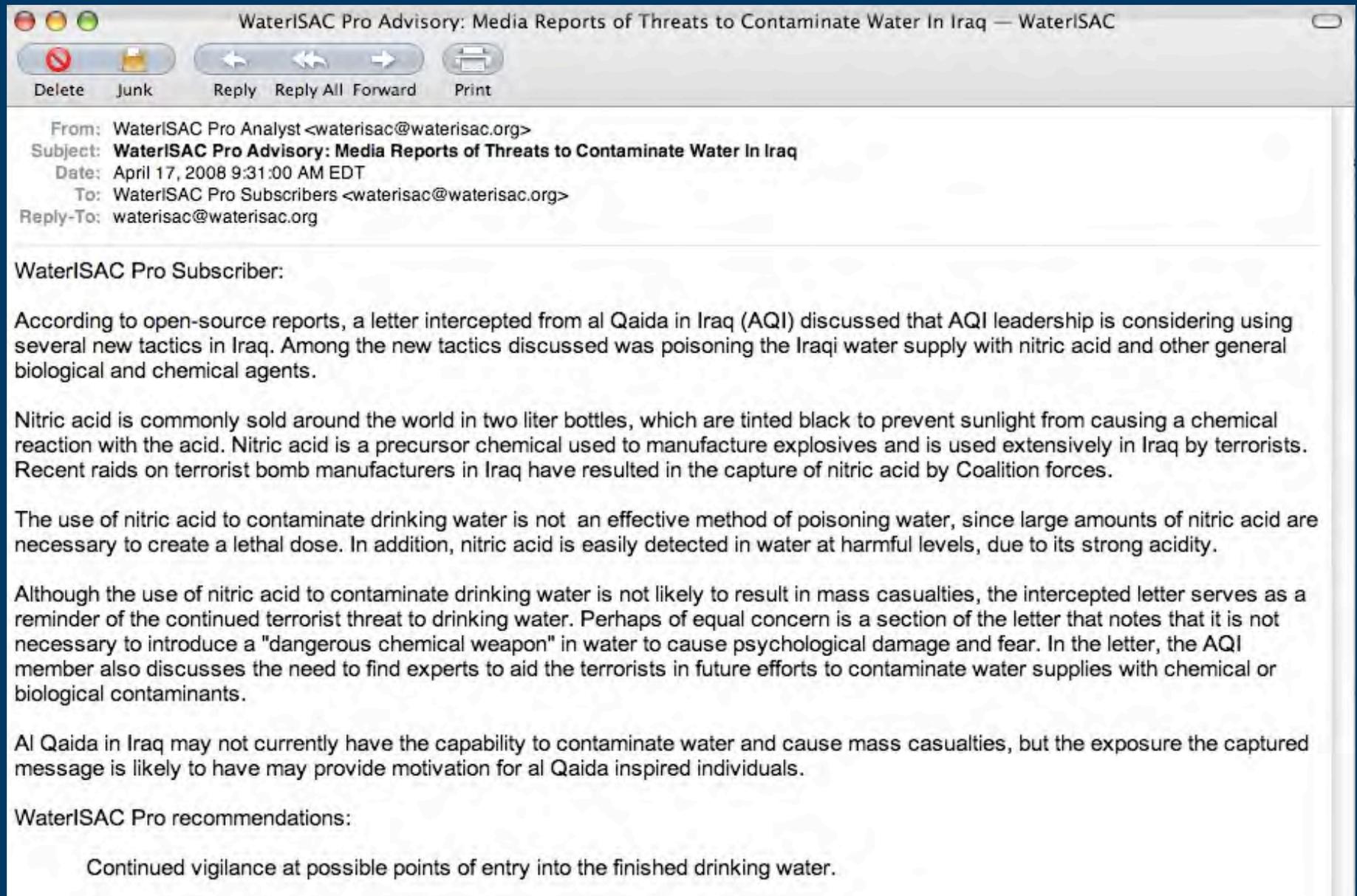


WaterISAC

WaterISAC Cyber Attack Trends

- ✓ Cyber attacks against the U.S. water infrastructure are a serious potential threat.
- ✓ In general, the majority of worldwide cyber attacks appear to originate from within the United States. However, the attacks could be launched by entities abroad who launch their attacks using hijacked computers in the U.S.
- ✓ China currently ranks second for worldwide cyber attacks. Chinese entities have publicized their cyber attack capabilities in open-source reporting.
- ✓ Attackers infiltrate computers using network service ports and, more recently, specialized "backdoor" tool ports used for legitimate business applications.

WaterISAC Pro E-Mail Alert



The image shows a screenshot of an email client window. The title bar reads "WaterISAC Pro Advisory: Media Reports of Threats to Contaminate Water In Iraq — WaterISAC". The window contains a standard email header with fields for From, Subject, Date, To, and Reply-To. The main body of the email is a text-based advisory. The text discusses a letter intercepted from al Qaida in Iraq (AQI) regarding threats to contaminate water with nitric acid and other agents. It explains that nitric acid is commonly used in Iraq by terrorists and that the use of nitric acid to contaminate drinking water is not an effective method of poisoning. The advisory concludes with a recommendation for continued vigilance at possible points of entry into finished drinking water.

From: WaterISAC Pro Analyst <waterisac@waterisac.org>
Subject: **WaterISAC Pro Advisory: Media Reports of Threats to Contaminate Water In Iraq**
Date: April 17, 2008 9:31:00 AM EDT
To: WaterISAC Pro Subscribers <waterisac@waterisac.org>
Reply-To: waterisac@waterisac.org

WaterISAC Pro Subscriber:

According to open-source reports, a letter intercepted from al Qaida in Iraq (AQI) discussed that AQI leadership is considering using several new tactics in Iraq. Among the new tactics discussed was poisoning the Iraqi water supply with nitric acid and other general biological and chemical agents.

Nitric acid is commonly sold around the world in two liter bottles, which are tinted black to prevent sunlight from causing a chemical reaction with the acid. Nitric acid is a precursor chemical used to manufacture explosives and is used extensively in Iraq by terrorists. Recent raids on terrorist bomb manufacturers in Iraq have resulted in the capture of nitric acid by Coalition forces.

The use of nitric acid to contaminate drinking water is not an effective method of poisoning water, since large amounts of nitric acid are necessary to create a lethal dose. In addition, nitric acid is easily detected in water at harmful levels, due to its strong acidity.

Although the use of nitric acid to contaminate drinking water is not likely to result in mass casualties, the intercepted letter serves as a reminder of the continued terrorist threat to drinking water. Perhaps of equal concern is a section of the letter that notes that it is not necessary to introduce a "dangerous chemical weapon" in water to cause psychological damage and fear. In the letter, the AQI member also discusses the need to find experts to aid the terrorists in future efforts to contaminate water supplies with chemical or biological contaminants.

Al Qaida in Iraq may not currently have the capability to contaminate water and cause mass casualties, but the exposure the captured message is likely to have may provide motivation for al Qaida inspired individuals.

WaterISAC Pro recommendations:

Continued vigilance at possible points of entry into the finished drinking water.

www.WaterISAC.org

Home | WaterISAC - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Stop

Address <http://www.waterisac.org/> Go Links >>

Report An Incident | Contact Us

WaterISAC

Water Security Network

Enter keywords... Go

[What Is WaterISAC](#) [Who Needs WaterISAC](#) [WaterISAC Pro Services](#) [Case Studies](#) [Become a Subscriber](#) [Basic Subscribers](#) [WaterISAC Pro Login](#)

Welcome to WaterISAC

WaterISAC is the most comprehensive and up-to-the-minute online resource of security and disaster preparedness information for America's drinking water and wastewater utilities. It provides a unique link between the water sector and federal environmental, homeland security, law enforcement, intelligence and public health agencies.



WaterISAC Basic	WaterISAC Pro	Subscriber Login
<p>WaterISAC Basic is a free, rapid, email notification of water security alerts and other information issued by federal government agencies.</p> 	<p>WaterISAC Pro is a collection of all-hazards expertise and services designed to meet the requirements of forward-looking water and wastewater utilities.</p> 	<p>WaterISAC Users </p> <p>WaterISAC Users </p>

Our Purpose Is Security
Drinking water is a basic life resource and

Watch WaterISAC Video
The importance of drinking water

Alerts
Latest Alerts on WaterISAC Pro

WaterISAC Pro Secure Portal

The screenshot displays the WaterISAC Pro Secure Portal website. At the top left is the WaterISAC logo, featuring a star with water droplets and the text "WaterISAC Water Security Network". A navigation menu includes "WORKPLACES", "LIBRARY", "MY PROFILE", "RESOURCES", "CONTACTS", "PORTAL HELP", "NOTIFICATIONS", and "LOGOFF". A search bar is located on the right. Below the navigation is a breadcrumb trail: "Homepage | Bulletin Board | Chat Rooms". A dropdown menu for "All Workplaces" is set to "Homepage".

The main content area is divided into several sections:

- Threat Reporting:** Features a large heading "WHEN IN DOUBT, REPORT!" and sub-heading "Suspicious Activities, Threats, & Incidents". It includes links for "Easy Online Reporting Form", "Monthly Summary", "Quarterly Analysis", "Monthly Cyber Trends", "Suspicious Activity - What is it?", and "General Overview".
- What's New:** Contains a "Welcome to the WaterISAC Portal" message with a mission statement: "The mission of the WaterISAC is to provide drinking water and wastewater sharing security-related information. The WaterISAC will provide utilities protect critical water infrastructure." Below this are several news items with "click here" links, such as "US CERT CIIN - Imminent Spear Phishing Campaign - 2/1/08", "CIN - Al-Qaida Media Releases Continue - 1/30/08", "DHS - Cyber Attacks on Control Systems Overseas Portend No Homeland Threat", "CIN UPDATE - Extremists Arrested in Spain - 1/25/08", "FBI - Aviation Threat Assessment - 1/25/08", and "WaterISAC 2007 Terrorism and Security Year in Review - 1/24/08".
- CBR Databases:** Lists four databases: "EPA WCIT", "WaterISAC Biological and Chemical Toxin Database", "UK WIR Toxicity Datasheets", and "UK WIR Microbiology Datasheets".
- National Threat Level:** A section for monitoring the current threat level.
- Emergency Contacts:** A section for critical contact information.
- Ten Latest Notifications:** A table listing recent alerts and reports, including "WaterISAC Weekly Report 1/28/08 - 2/4/08", "WaterISAC Bulletin: US CERT CIIN - Imminent Spear Phishing Campaign", "WaterISAC Update: Announcing New WaterISAC Services", "WaterISAC Update: Additional Information Regarding Recent Website Hack", "WaterISAC Weekly Report 1/22/08 - 1/28/08", "WaterISAC Advisory: Foreign Hackers Targeting Websites of U.S. Water Facilities", "WaterISAC Bulletin: 2007 Terrorism and Security Year in Review", "WaterISAC Weekly Report 1/14/07 - 1/22/08", and "WaterISAC Update: Monthly Cyber Trends Report".

Searching the Library

WaterISAC - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites RSS Print Mail News Groups

Address <https://subscribers.waterisac.org/servlet/portal?SESSION=bgjIQZpOGnMTost175> Go

WaterISAC Information Sharing & Analysis Center

[WORKPLACES](#) | [LIBRARY](#) | [MY PROFILE](#) | [RESOURCES](#) | [CONTACTS](#) | [PORTAL HELP](#) | [NOTIFICATIONS](#) | [LOGOFF](#) SEARCH

SEARCH

Search For:

Search Type:

Keywords and/or Author:

Title: Search for Document Title, library folder (Full or Partial)

Filename: Search for document by computer file name

Constrain By:

Create Date: (Dates = Month / Day / Year)

All

Date Range

From:
Month: Day: Year:

To:
Month: Day: Year:

Inside a WaterISAC Pro Folder

The screenshot shows a Windows Internet Explorer browser window with the URL <https://subscribers2.waterisac.org/servlet/portal?escmd=startup&SESSION=1cd280b:116ef0feb7a:-2e2b:nile:10.1.5.55>. The page header includes the WaterISAC logo and the text "Information Sharing & Analysis Center". Below the header is a navigation menu with links for WORKPLACES, LIBRARY, MY PROFILE, RESOURCES, CONTACTS, PORTAL HELP, NOTIFICATIONS, and LOGOFF. A search bar is located on the right side of the navigation menu.

The main content area is divided into two sections: "Channels" and "Library". The "Library" section is expanded, showing a list of channels. The "Content" section is also expanded, showing a table of content items. The table has columns for "Select", "Name", "Size", "Postings", "Date", and "Options".

Select	Name	Size	Postings	Date	Options
<input type="checkbox"/>	EXERCISE Weekly		0	10/12/07	
<input type="checkbox"/>	(U//EX//FOUO) EXERCISE TOPOFF 4: Explosion near	15k	0	10/16/07	
<input type="checkbox"/>	EPA Threat Level Guidance	215k	0	10/17/07	
<input type="checkbox"/>	EXERCISE - Detonation of Radiological Dispersal Device DHS Situation Report 586k (SITREP)		0	10/17/07	
<input type="checkbox"/>	EXERCISE - GUARDING AGAINST TERRORIST AND SECURITY THREATS	215k	0	10/17/07	
<input type="checkbox"/>	Exercise - Portland OR - Detonation of Radiological Dispersal Device DHS Situation Report (SITREP)	628k	0	10/17/07	
<input type="checkbox"/>	EXERCISE - Sheltering in Place - Oregon DHS	33k	0	10/17/07	
<input type="checkbox"/>	EXERCISE - THREAT ADVISORY SYSTEM RESPONSE (TASR) DRAFT GUIDELINE	268k	0	10/17/07	
<input type="checkbox"/>	EXERCISE Guam Detonation of Radiological Dispersal Device	137k	0	10/17/07	

The "Channels" section includes the following items:

- 14 Features
- AwwaRF Research
- Blast Vulnerability Assessment T
- Bulletin Board
- Chat Rooms
- Contaminants
- Contamination Monitors
- Cyber SCADA
- DHS Security Programs
- Emergency Response
- EPA Threat Documents
- F&T
- Government and Law Enforcement
- Hurricane Season 2006
- Hurricane Season 2007
- Incident Reporting
- International Portal Content
- Legal Issues
- Mutual Aid Agreements
- Open Source Intelligence
- Pandemic
- PipelineNet RiverSpill
- Portal Content
- Private Sector Intelligence
- Public Policy
- Research in Progress
- Security Practices
- Threat Level Practices
- TOPOFF 4 Exercise
- TOPOFF 4 Facilities
- Training Aids
- Virtual Meetings
- VSAT
- Vulnerability Assessments

WaterISAC Pro Bulletin

https://subscribers2.waterisac.org/servlet/portal/serve/Library/WaterISAC%20Advisories/Summer%20Threat-Water.pdf - Microsoft Internet Explorer

File Edit Go To Favorites Help

Back Home Search Favorites

Address https://subscribers2.waterisac.org/servlet/portal/serve/Library/WaterISAC%20Advisories/Summer%20Threat-Water.pdf Go Links

1 / 3 101% Find



16 July 2007

WaterISAC Analysis: Summer Threat Reported In the Media

Bottom Line Upfront:

- Al Qaida remains determined to conduct terrorist attacks against the United States.
- Open source information indicates that an unspecified credible threat against the United States exists for the summer of 2007.
- Authorities have used communications from the suspected London Bombers to decode other messages that reveal information about terrorist operations against the United States.
- Global terrorism trends and recent plots/attacks indicate that summer is the preferred season to conduct terrorist attacks against the West.

Introduction:

A DHS Bulletin on “Dirty Bombs”

https://subscribers2.waterisac.org/servlet/portal/serve/3509/Joint%20DHS-DOE%20Red%20Cell%20-%2 - Microsoft Internet Explorer

File Edit Go To Favorites Help

Back Search Favorites

Address https://subscribers2.waterisac.org/servlet/portal/serve/3509/Joint%20DHS-DOE%20Red%20Cell%20-%20How%20Terrorist%20Might%20Use%20Dirty%20Bomb%20.pdf Go

Layers Pages Attachments

UNCLASSIFIED//FOR OFFICIAL USE ONLY

 Information Analysis and Infrastructure Protection, Department of Homeland Security

 Office of Intelligence, Department of Energy

IAIP Analytic Red Cell Program 

How Terrorists Might Use a “Dirty Bomb” Against the Homeland

LIMITED DISTRIBUTION: Any release, dissemination, or sharing of this document, or any information contained herein, is not authorized without approval from the Department of Homeland Security (DHS). Release to Intelligence Community is authorized. All requests for further dissemination outside of Intelligence Community entities must be approved by the DHS, Information Analysis - Requirements Division at DHS.IAIP@hq.dhs.gov.

October 13, 2004

Project Overview

A Red Cell session was held jointly by the US Departments of Energy and Homeland Security on 8 June 2004 to examine the prospects of a RDD attack on the U.S. homeland. The 17 participants emulated terrorist cells, dividing into a “poorly

Summary: An independent, unclassified analytic Red Cell session, sponsored jointly by the U.S. Departments of Energy and Homeland Security, found a Radiological Dispersal Device (RDD) attack on the

WaterISAC: Not Just About Terrorism

Adobe Reader - [panflu_chlorine_nrc] (1).pdf

File Edit View Document Tools Window Help

Save a Copy Search Select 150% Help Search Web Download New Reader Now

Chlorine Inactivation of Highly Pathogenic Avian Influenza Virus (H5N1)

Eugene W. Rice,* Noreen J. Adcock,* Mano Sivaganesan,* Justin D. Brown,†
David E. Stallknecht,† and David E. Swayne‡

*US Environmental Protection Agency, Cincinnati, Ohio, USA; †University of Georgia, Athens, Georgia, USA; and
‡US Department of Agriculture, Athens, Georgia, USA

To determine resistance of highly pathogenic avian influenza (H5N1) virus to chlorination, we exposed allantoic fluid containing 2 virus strains to chlorinated buffer at pH 7 and 8, at 5°C. Free chlorine concentrations typically used in drinking water treatment are sufficient to inactivate the virus by >3 orders of magnitude.

Growing concerns about the public health threat posed by highly pathogenic avian influenza (HPAI) subtype H5N1 has prompted interest in evaluating environmental control measures for this virus. The World Health Organization has noted that more information is needed on the effectiveness of inactivation of subtype H5N1 in water (1). Since 2002, HPAI

WaterISAC Relies on Many Sources

SURVIVING THE NEXT BLACKOUT

THE CLEVELAND DIVISION OF WATER'S POWER OUTAGE OPTIONS



UK WIR Contaminant Database

UKWIR - Toxicity Datasheets - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Forward

Address https://www.ukwir.org/toxicity/default_cms.asp Go Links >>

WATERISAC

Information Sharing & Analysis Center

Back Stop Forward

Select a Datasheet

- Welcome Page
- Background & Derivations
- View SNARL's
- Latest Newsletter
- Datasheet Search
- Feedback Form
- Glossary
- Document Archive

Welcome to "Toxicity Datasheets"

UKWIR's Database on Chemical Toxicity, Environmental Fate and Water Treatment

Toxicity Datasheets has been developed to provide information to assist water suppliers and other users to respond in a rapid and effective manner to water pollution incidents. The database has been compiled over many years and is the largest of its kind. It is maintained by WRc plc on behalf of UK Water Industry Research (UKWIR) and contains a wealth of information on over 500 chemicals including:

- Occurrences and likely sources / uses of chemicals
- Human and mammalian toxicity data
- Health-based and / or operational SNARL values (Suggested No Adverse Response Levels)
- Toxicity for aquatic life
- Taste and odour
- Removal during water and wastewater treatment
- Analytical methods and detection limits

The user has access to comprehensive information for many chemicals in the Toxicity Datasheets. However, in the event that additional data are required, assistance can be requested from WRc plc through the Toxicity Advisory Service. This service is provided 24 hours a day, 365 days a year and is **free to UKWIR members** (Contact WRc's UKWIR toxicity advisory service on:- 0800 3897888). The staff will be happy to assist in locating data and/or in its interpretation. There is a charge to **non-UKWIR**

Version 2
[07/TX/01/19]
Internet Version

Managed Edition

EPA's WCIT Contaminant Data

WCIT Contaminant Index - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address https://cdx.epa.gov/SSL/WCIT/wtAgent_Index.cfm Go Links

WCIT WATER CONTAMINANT INFORMATION TOOL HOME | HELP | LOG OUT

SEARCH CONTAMINANT INDEX TOOLS FEEDBACK

Contaminant Index

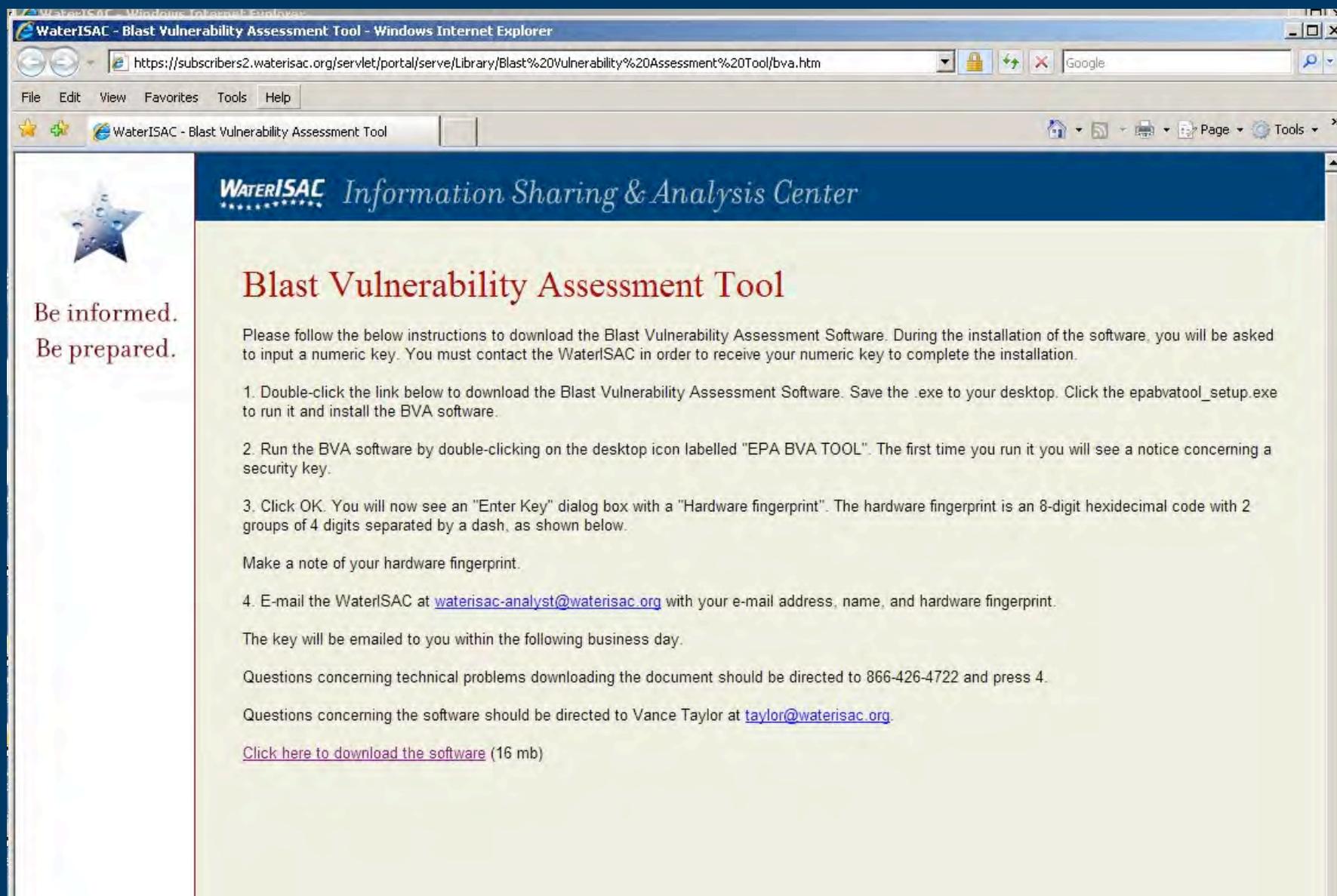
The contaminant index lists all contaminants and formulations currently in WCIT. Click on a contaminant name to view the corresponding contaminant profile. If the name is a formulation, the profile for the corresponding parent contaminant will be displayed. To sort the data, click on the arrows adjacent to the contaminant name, category, or public health threat index column headings. The arrow pointing up (▲) conducts an ascending sort; the arrow pointing down (▼), a descending sort. Click a letter of the alphabet to jump to the contaminant names beginning with that letter, or use the navigation buttons to view the data in sets of 30.

NOTE: Public health threat index analysis is ongoing. Data are forthcoming.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) 1 to 30 of 93

Name ▲	Category ▲	Public Health Threat Index ▲	Threat Categories
Abrin	Biotoxin		Environmental, Infrastructure, Public Health
Acrolein	Organic		Environmental, Public Health
Aflatoxin	Biotoxin		Environmental, Public Health
Aldicarb	Organic		Environmental, Public Health

Only on WaterISAC Pro



The screenshot shows a Windows Internet Explorer browser window. The address bar contains the URL: <https://subscribers2.waterisac.org/servlet/portal/serve/Library/Blast%20Vulnerability%20Assessment%20Tool/bva.htm>. The browser title is "WaterISAC - Blast Vulnerability Assessment Tool". The page content includes the WaterISAC logo and the text "Information Sharing & Analysis Center". The main heading is "Blast Vulnerability Assessment Tool". The page provides instructions for downloading and installing the software, including a list of steps and contact information for technical support.

WaterISAC Information Sharing & Analysis Center

Blast Vulnerability Assessment Tool

Please follow the below instructions to download the Blast Vulnerability Assessment Software. During the installation of the software, you will be asked to input a numeric key. You must contact the WaterISAC in order to receive your numeric key to complete the installation.

1. Double-click the link below to download the Blast Vulnerability Assessment Software. Save the .exe to your desktop. Click the epabvatool_setup.exe to run it and install the BVA software.
2. Run the BVA software by double-clicking on the desktop icon labelled "EPA BVA TOOL". The first time you run it you will see a notice concerning a security key.
3. Click OK. You will now see an "Enter Key" dialog box with a "Hardware fingerprint". The hardware fingerprint is an 8-digit hexadecimal code with 2 groups of 4 digits separated by a dash, as shown below.

Make a note of your hardware fingerprint.

4. E-mail the WaterISAC at waterisac-analyst@waterisac.org with your e-mail address, name, and hardware fingerprint.

The key will be emailed to you within the following business day.

Questions concerning technical problems downloading the document should be directed to 866-426-4722 and press 4.

Questions concerning the software should be directed to Vance Taylor at taylor@waterisac.org.

[Click here to download the software](#) (16 mb)



WaterISAC

Two Examples of WaterISAC's Value

1. Ricin found in a hotel room near a water treatment facility. The press and consumers want a response from the mayor.
2. Damage and flooding from Hurricane Katrina caused most of the New Orleans water and sewerage system to fail.



WaterISAC

Summary

1. WaterISAC is designed specifically for the water sector.
2. WaterISAC is the only resource of its kind with a national reach and its own intelligence analysts.
3. WaterISAC Pro has resources for utilities to address security threats and the impacts of natural disasters.



WaterISAC

[The water sector] has probably one of the best information-sharing networks . . . across our sectors.

-Col. Robert Stephan (ret.)
DHS Asst. Secretary for Infrastructure Protection
February 26, 2008



WaterISAC

For More Information

- ✓ Sign up for an online tour of WaterISAC at WaterISAC.org.
- ✓ Download a brochure from the WaterISAC website.
- ✓ Call 1 (866) H2O-ISAC.

* * *

- ✓ Every utility and state water/wastewater agency should have at least one manager with WaterISAC access.
- ✓ *Subscribe ONLINE at WaterISAC.org today.*