WaterISAC

Water Security Network

www.WaterISAC.org

WaterISAC

What is WaterISAC?

- ✓ ISAC = **I**nformation **S**haring & **A**nalysis **C**enter
- ✓ 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
	Highly sensitive information, which the WaterISAC security team analyzes prior to dissemination. • 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 *highly sensitive* 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

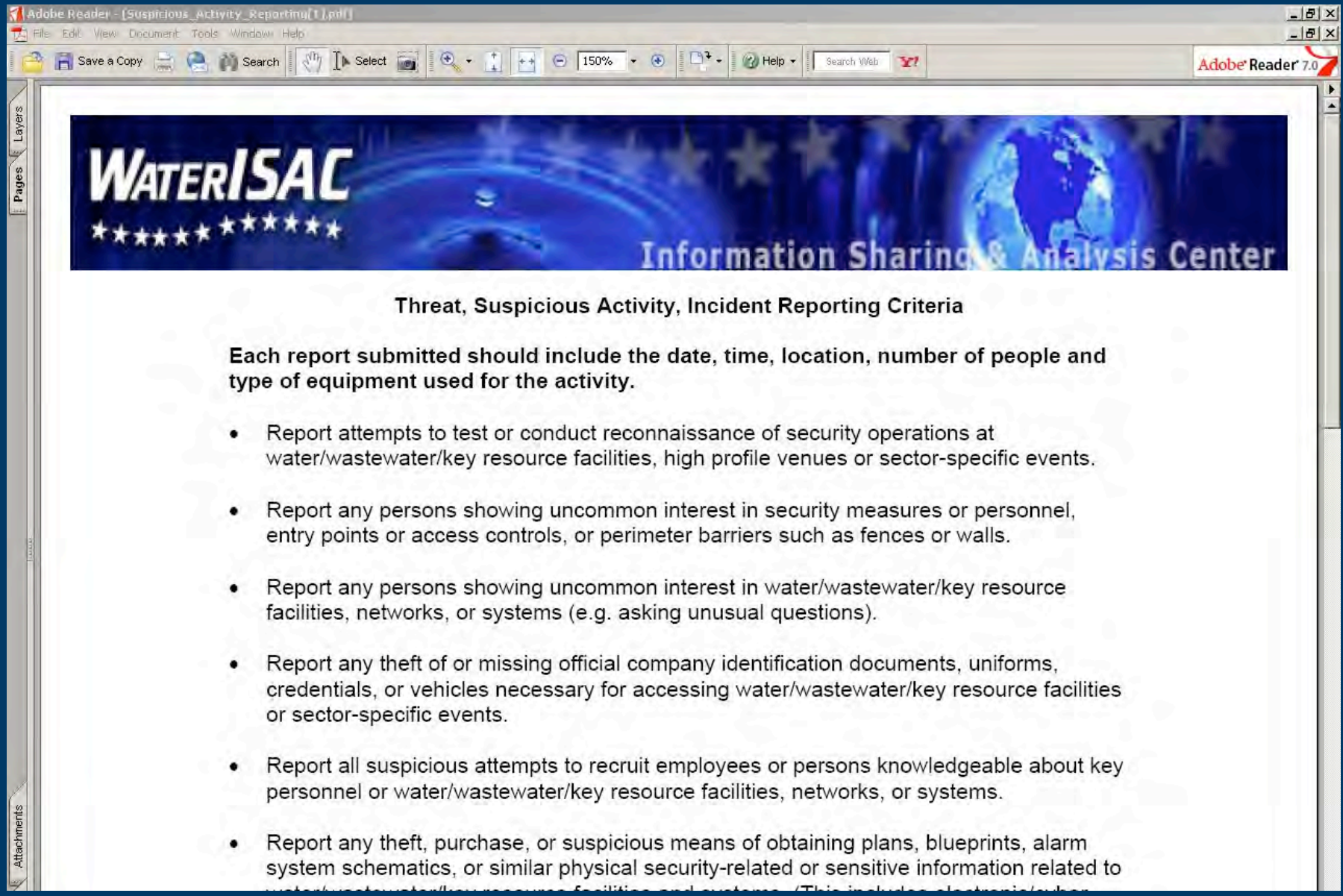
- ✓ Has a 24/7 team of intelligence analysts, who have federal TOP SECRET clearances.
- ✓ Delivers threat information by email and text messaging.
- ✓ Hosts a secure forum for collaboration.
- ✓ Helps subscribers demonstrate due diligence.
- ✓ Exempt from the Freedom of Information Act.
- ✓ Protects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

WaterISAC

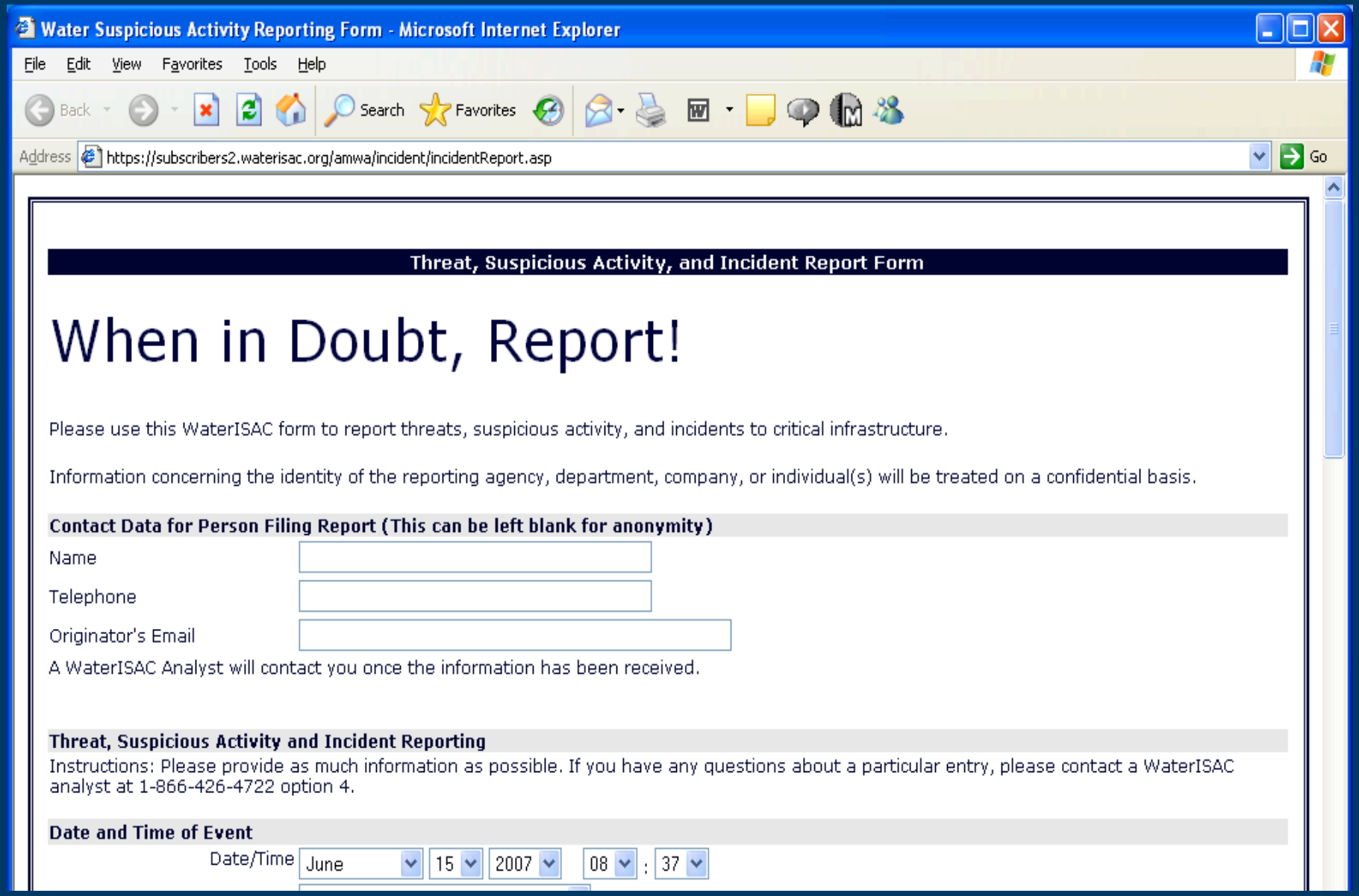
Intel and Information Partners

- ✓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



Incident, Suspicious Activity Reporting



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.

Monthly Cyber Attack Trends

WaterISAC

WaterISAC

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	15.79%	2	13.64%	2	15.41%

Cyber

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

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

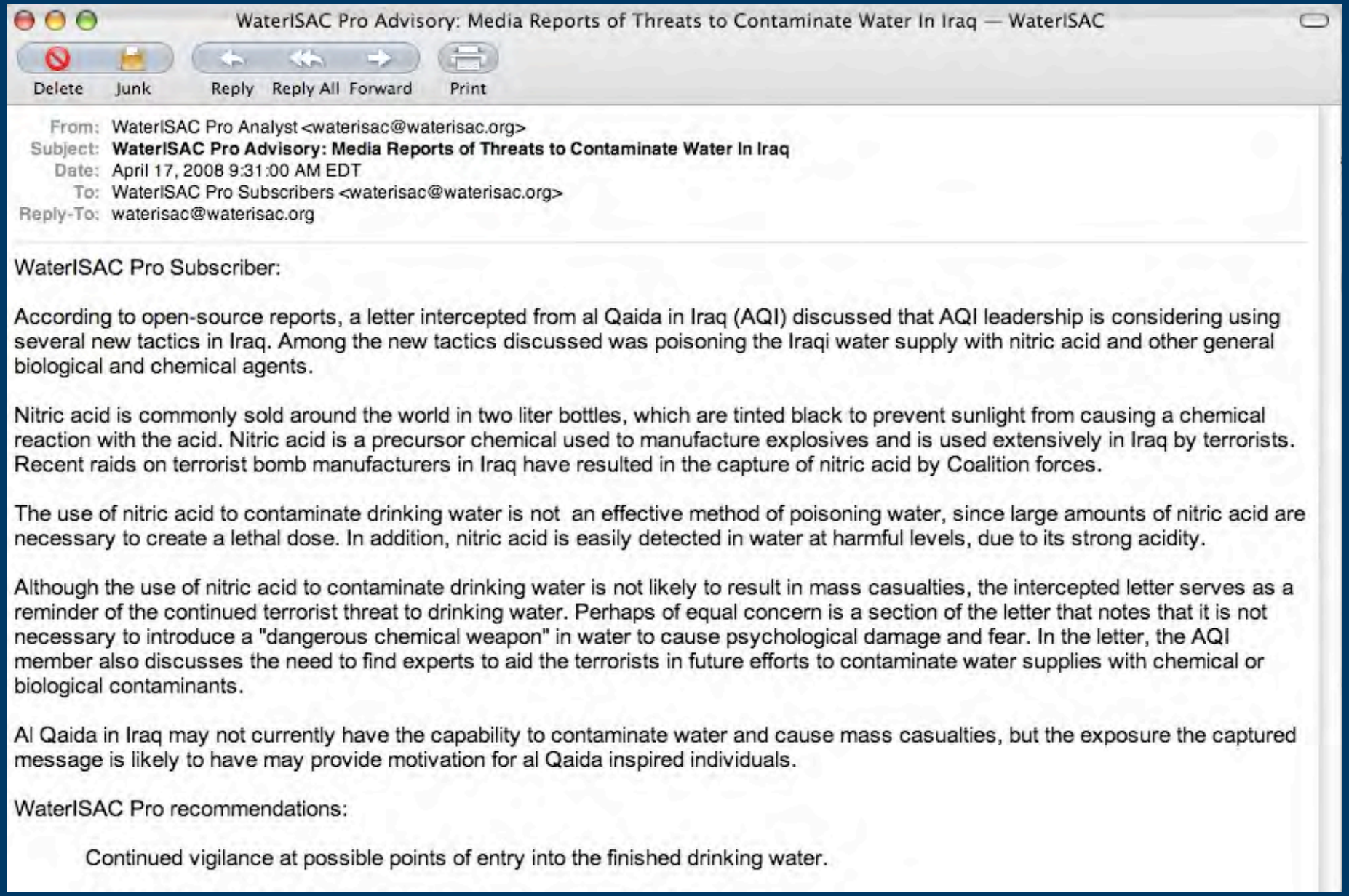
The above table provides a comparison of the EWA-Canada/CanCERT™ sensor top 10 ports and protocols along with a comparison to the previous month and the total for the previous six months.

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



WaterISAC Pro Advisory: Media Reports of Threats to Contaminate Water In Iraq — WaterISAC

Delete Junk Reply Reply All Forward Print

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.

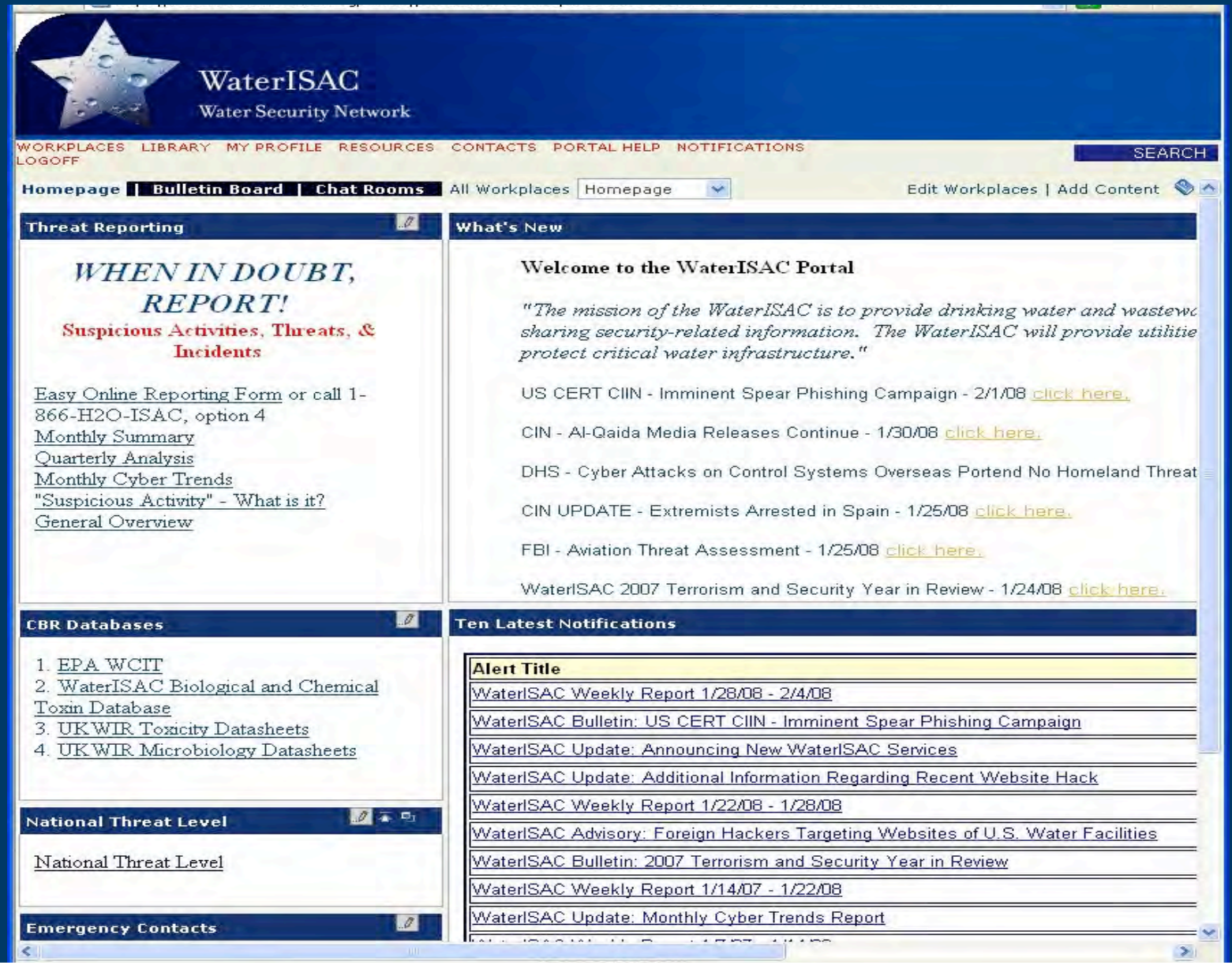
Al Qaida in Iraq may not currently have the capability to contaminate water and cause mass casualties, but the exposure the captured message is likely to have may provide motivation for al Qaida inspired individuals.

WaterISAC Pro recommendations:

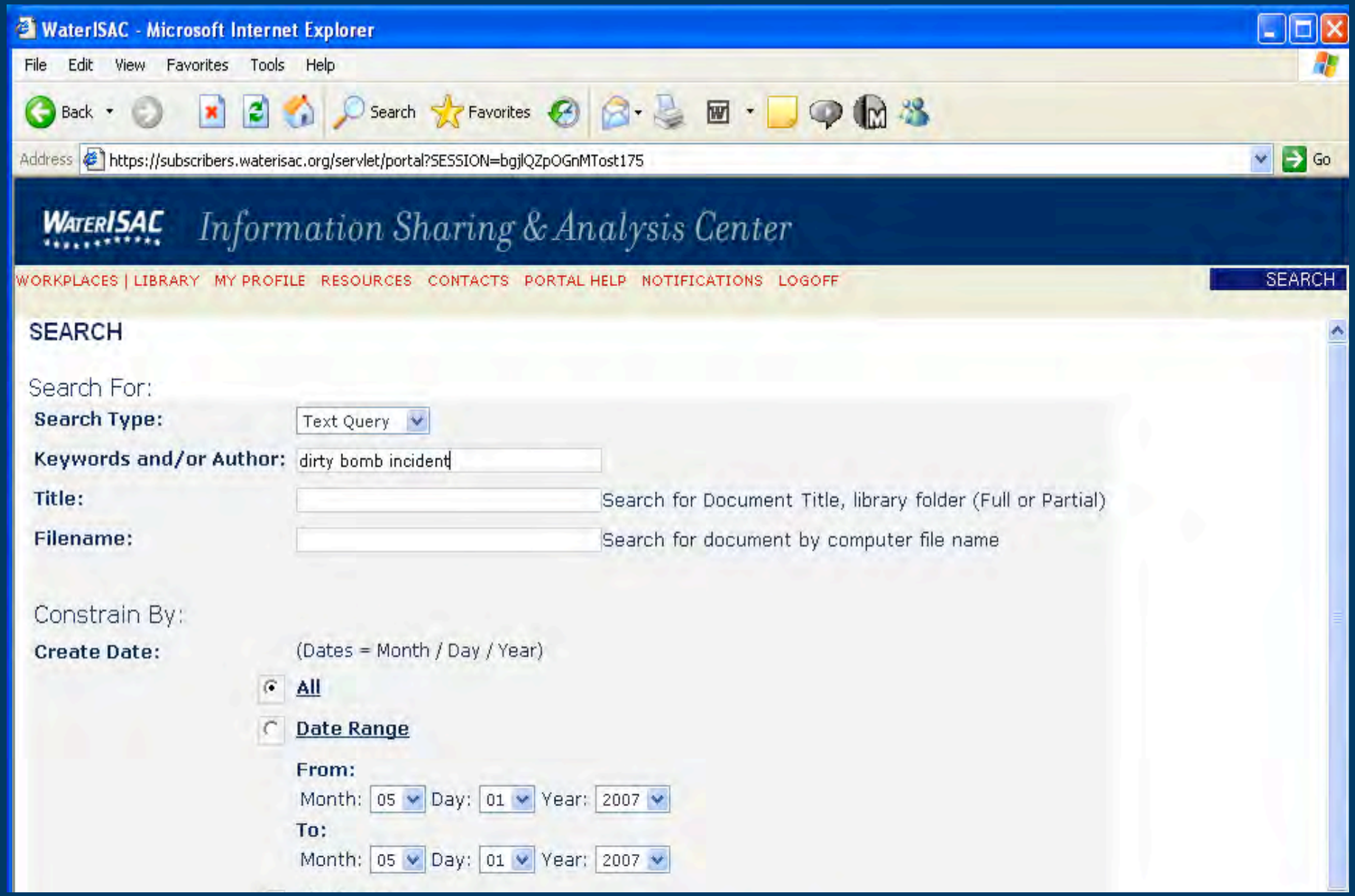
Continued vigilance at possible points of entry into the finished drinking water.

www.WaterISAC.org

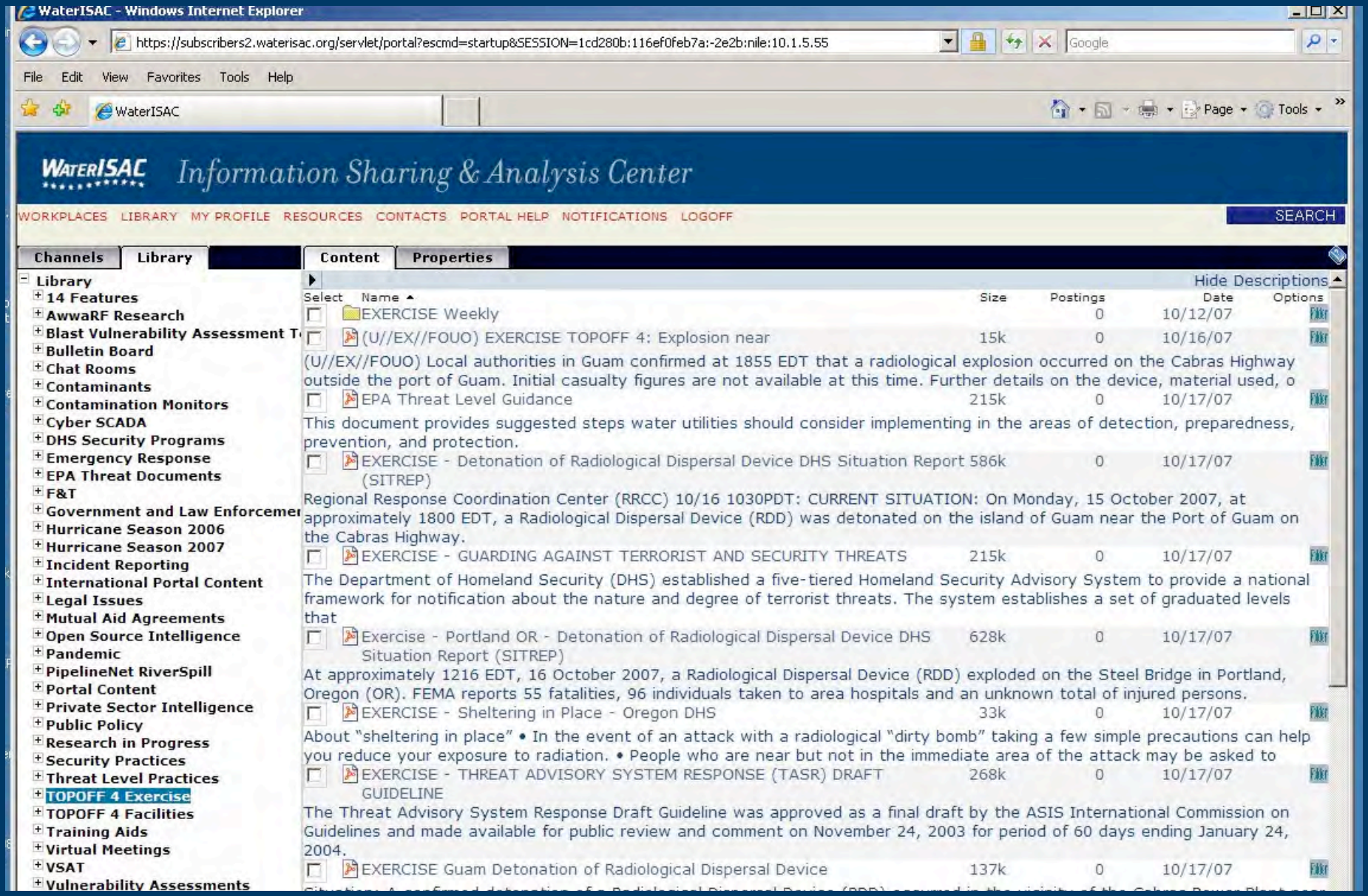
WaterISAC Pro Secure Portal



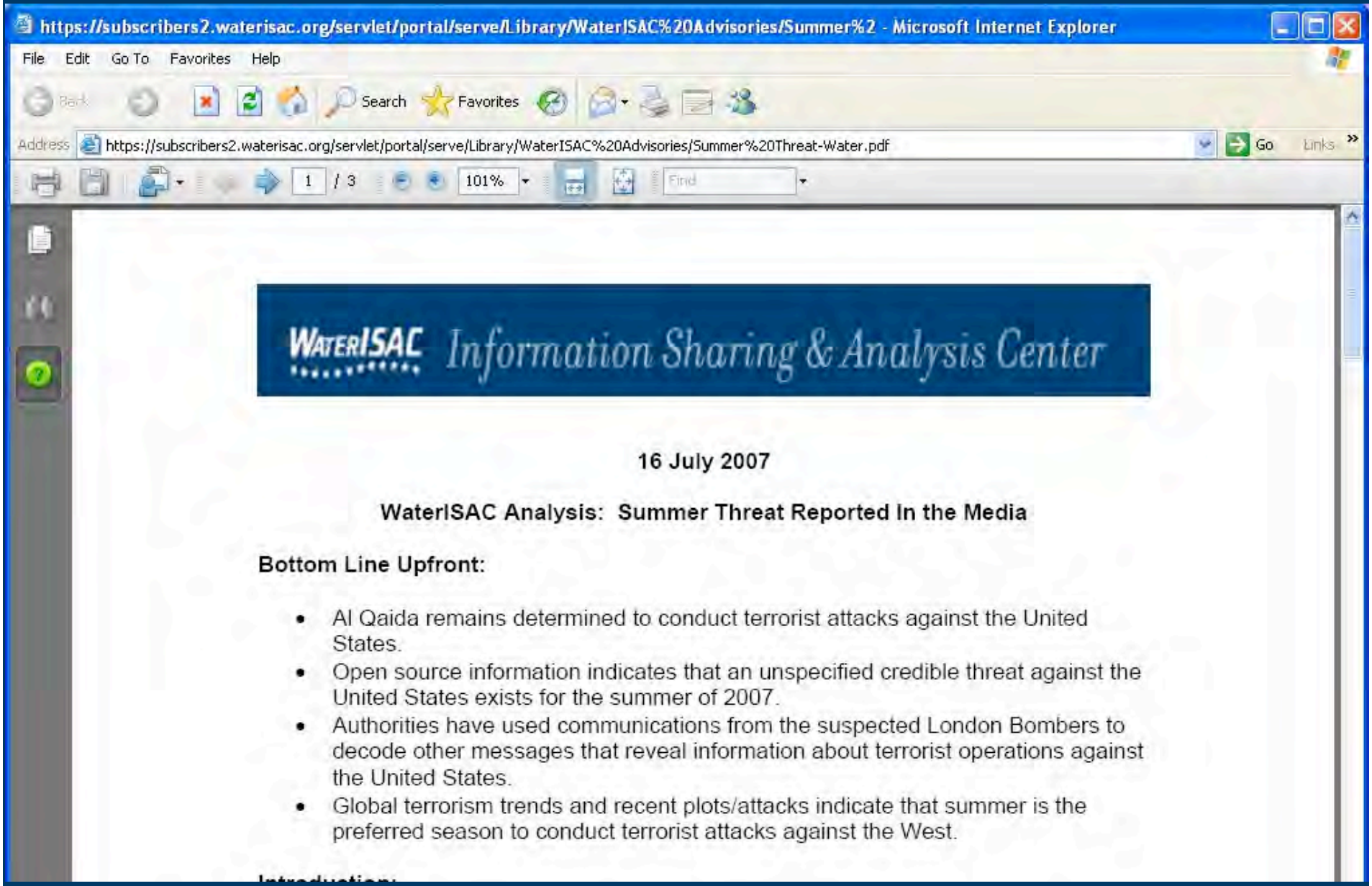
Searching the Library



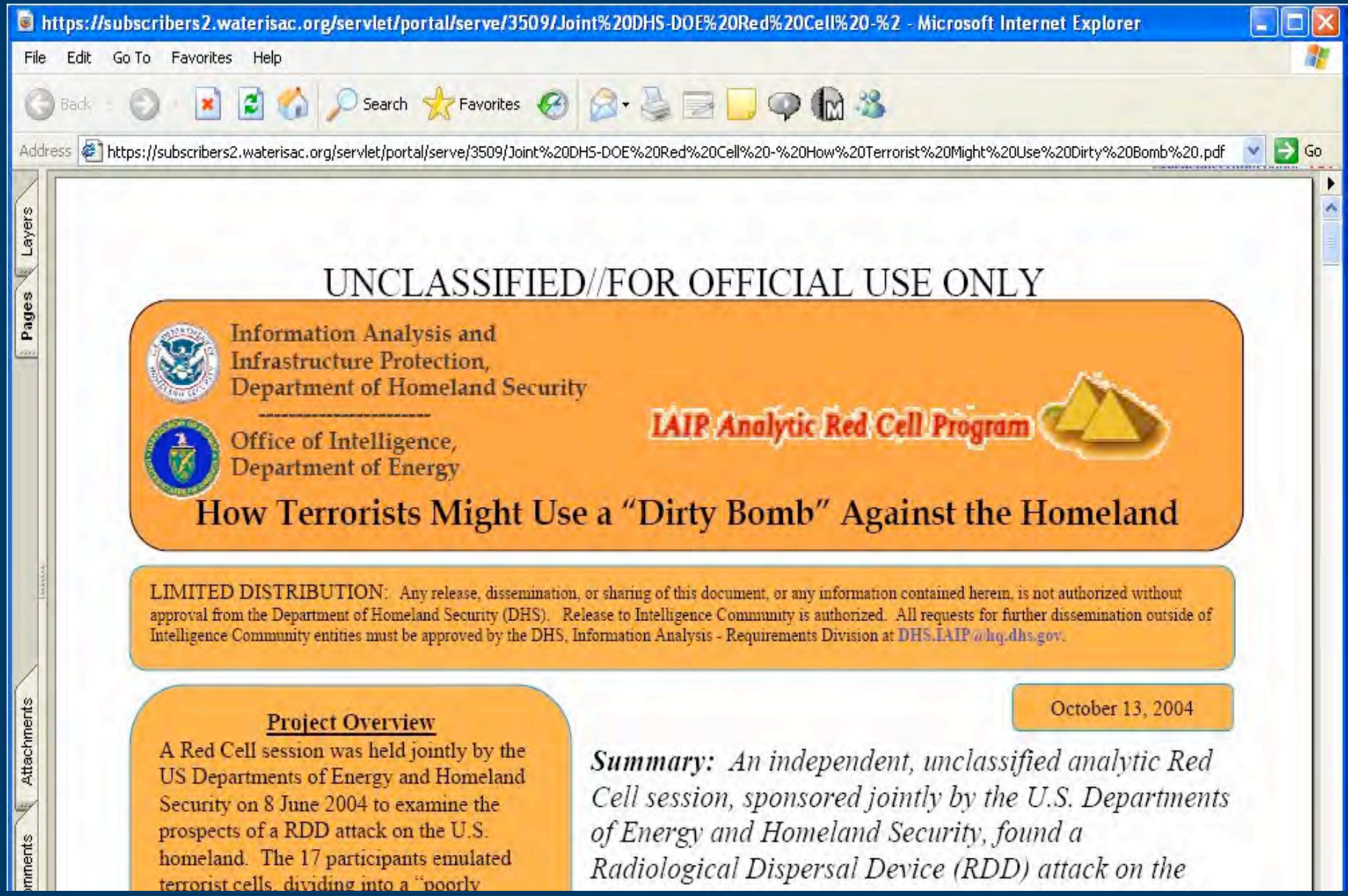
Inside a WaterISAC Pro Folder



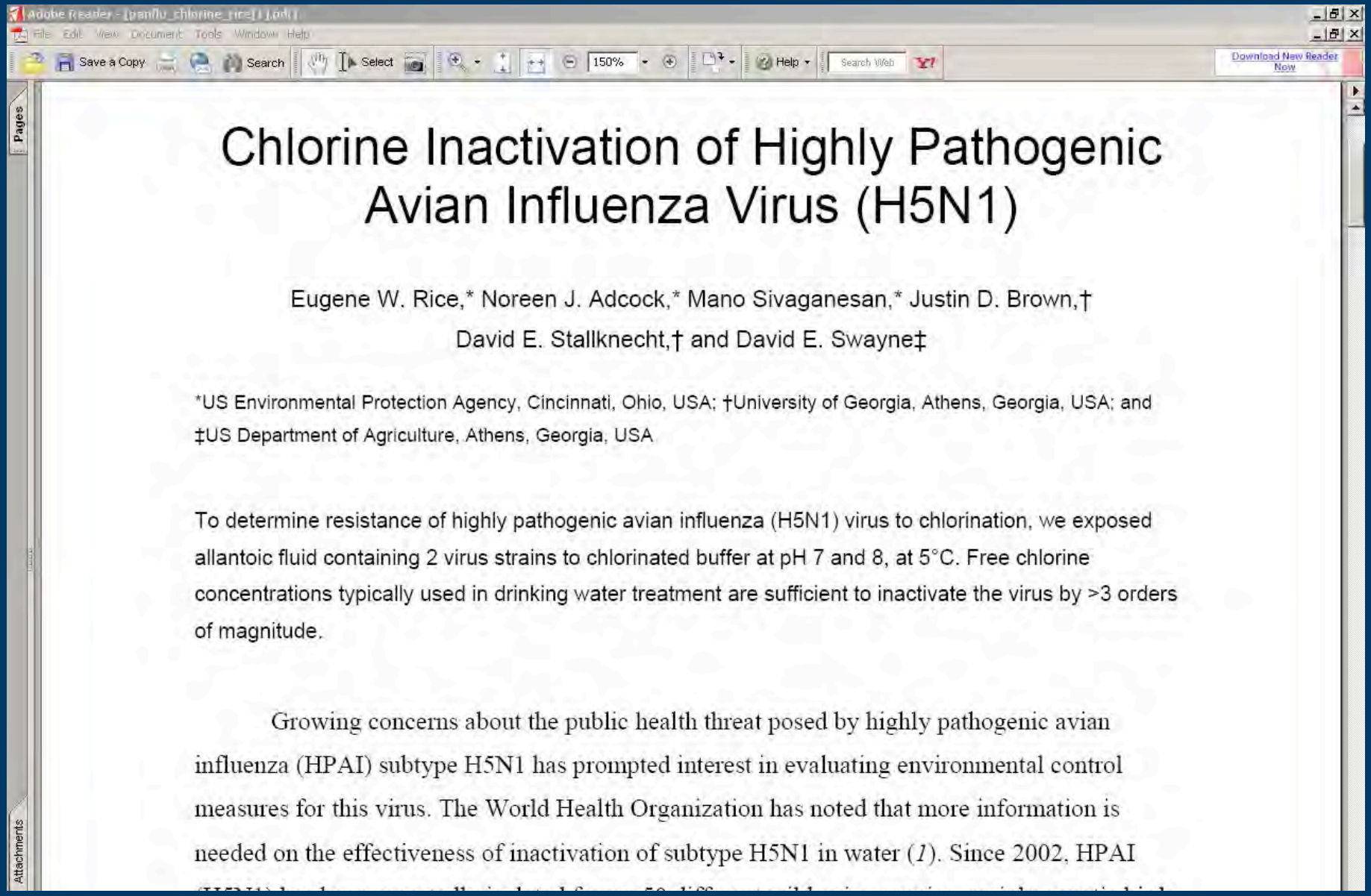
WaterISAC Pro Bulletin



A DHS Bulletin on “Dirty Bombs”



WaterISAC: Not Just About Terrorism



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

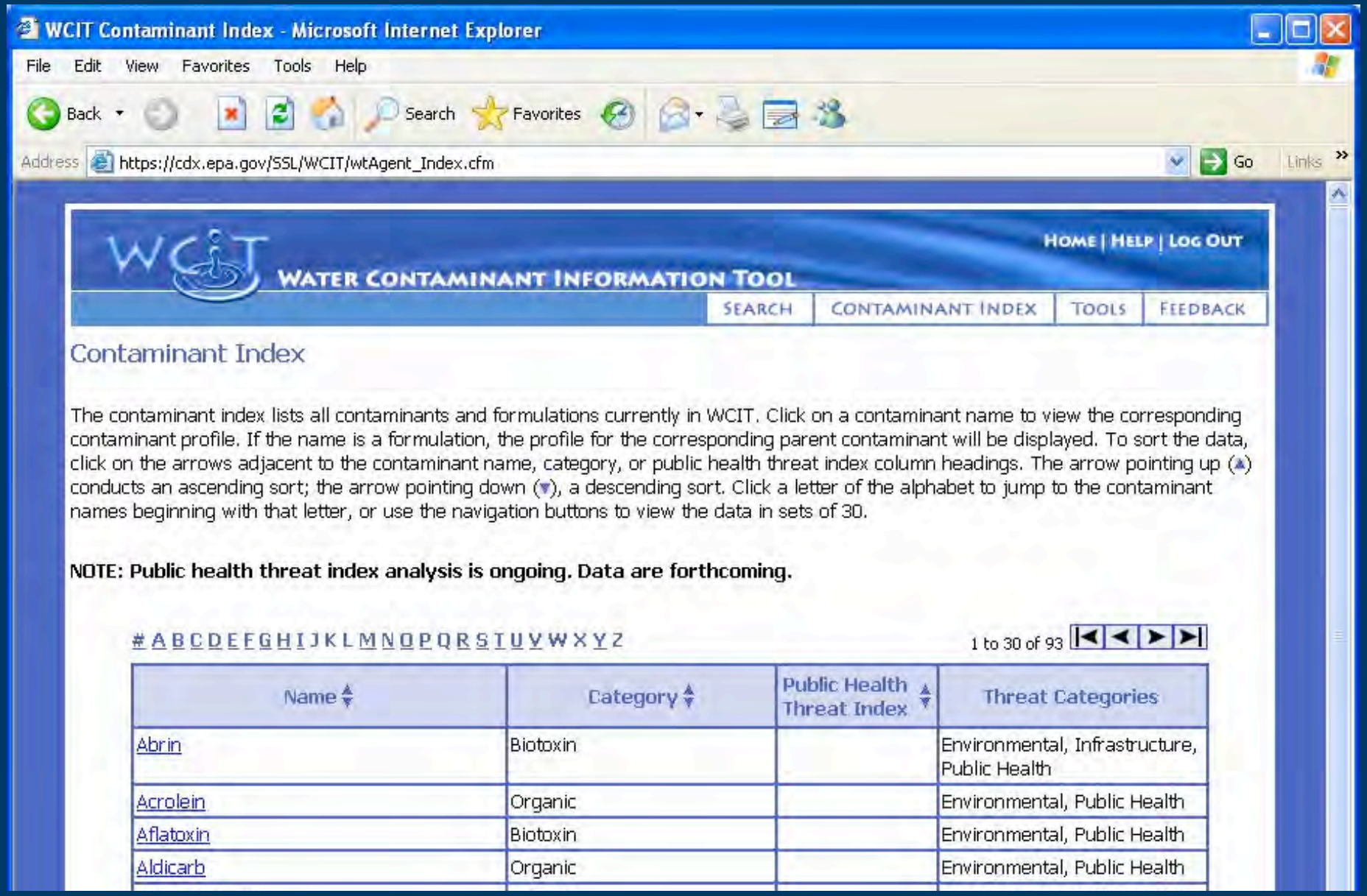
WaterISAC Relies on Many Sources

SURVIVING THE NEXT BLACKOUT

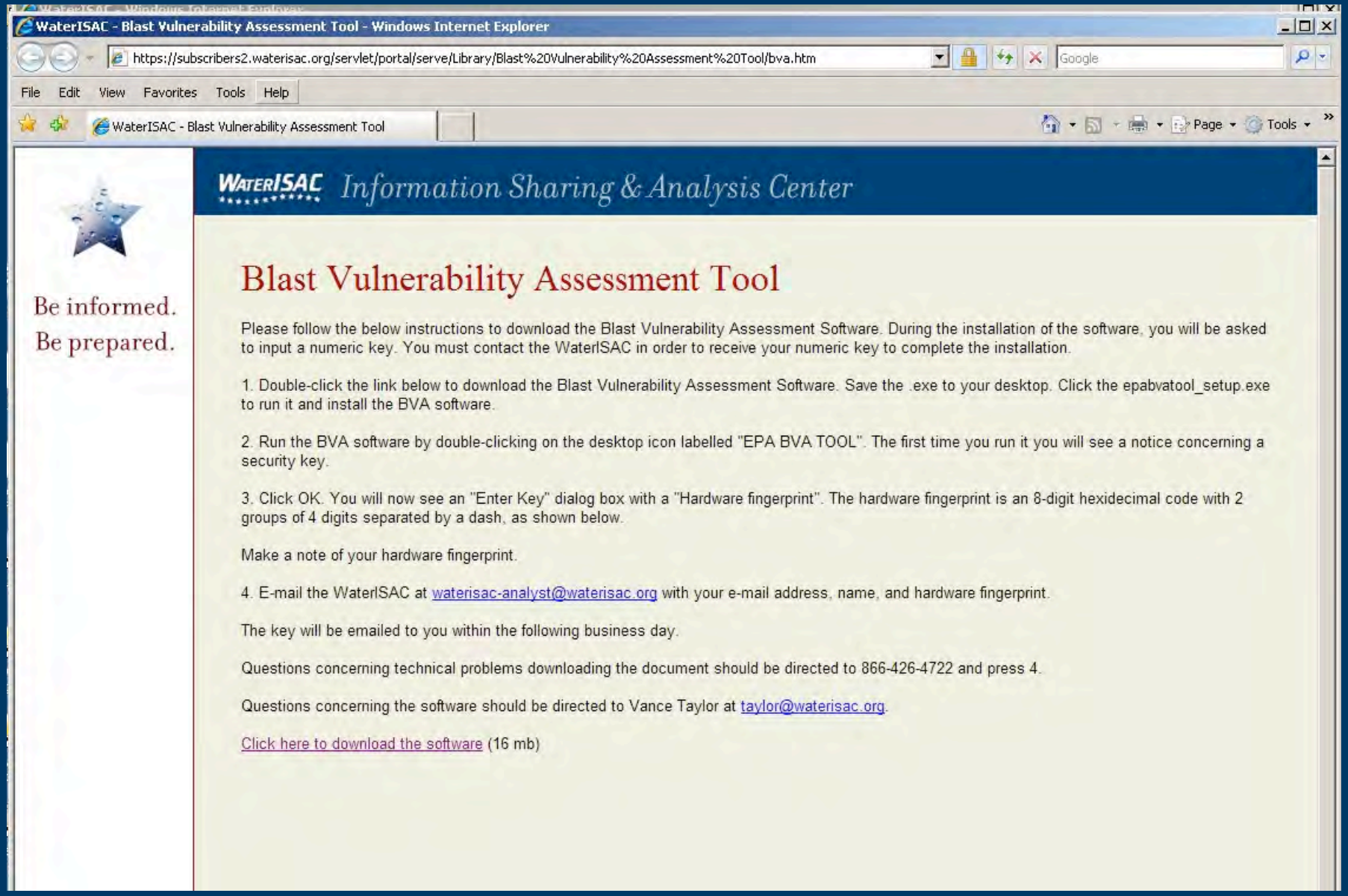
THE CLEVELAND DIVISION OF WATER'S POWER OUTAGE OPTIONS

UK WIR Contaminant Database

EPA's WCIT Contaminant Data



Only on WaterISAC Pro



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.*