The InfraGard Community
presented by Norman Arendt, PhD
Short Elliott Elliott Hendrickson (SEH)
Protect, Participate, Learn

OUR INFRASTRUCTURE
ENHANCED NETWORKING
ESSENTIAL INFORMATION
Nationally over 28,000 members
Public / Private Collaboration for National Infrastructure Protection
Strength is Subject Matter Expertise represented in Membership
Trusted Resources -- All Members vetted by FBI
Information Sharing and Security Awareness
MOU’s with many Federal and State Agencies
Three Chapters in the State of Wisconsin with over 300 members

Working on a MOU with WI Office of Homeland Security

- Milwaukee
- Madison
- Green Bay (2009)
- Eau Claire (Maybe)
In existence since 2000 in Western Wisconsin

100+ current members

Membership is a representation of Information Technology Subject Matter Experts, Physical Security Experts, Law Enforcement and First Responders
Infragard Purpose

*Mitigate Criminal- and Terrorist-based Threat, Risk and Loss*

- Provide opportunity to exchange ideas, information and security practices between the private sector, law enforcement, other first responders, government and academia.
- Provide members with timely threat/risk advisories, alerts and warnings.
- Provide a conduit to act as a “force multiplier” for the FBI and state/local law enforcement agencies
- Host regular meetings on timely topics of concern and importance to our critical infrastructure
Program Guidance

  - HSPD-7
  - Establishes CI/KR Program
- National Infrastructure Protection Plan (NIPP)
  - Guiding document for CIP
- Sector Specific Plans (SSP)
  - Guidance for individual sectors
- Intelligence Reform Act
  - Fusion centers
Homeland Security Presidential Directive-7 (HSPD-7) designates the Environmental Protection Agency (EPA) as the federal lead for the water/wastewater Sector's critical infrastructure protection activities. All activities are carried out in consultation with the Department and the EPA's water/wastewater Sector partners.

The water/wastewater Sector is vulnerable to a variety of attacks through contamination with deadly agents, physical attacks-such as the release of toxic gaseous chemicals-and cyber attacks. If these attacks were realized, the result could be large numbers of illnesses or casualties and/or a denial of service that would also impact public health and economic vitality. Critical services such as firefighting or healthcare and other dependent and interdependent sectors, such as Energy, Transportation Systems, and Agriculture and Food, would be negatively impacted by a denial of service from the water/wastewater Sector.
Infragard and the FBI

- Ask yourself;
  - What if there are no computers?
- Prevent and deter which means identify
  - FBI adds defeat
    - Pursue, prosecute
    - Provide crisis management
The Birth of Infragard

The National InfraGard Program began as a pilot project in 1996, when the Cleveland FBI Office asked local computer security professionals to assist the FBI in determining how to better protect critical information systems in the public and private sectors. From this new partnership, the first InfraGard Chapter was formed to address both cyber and physical threats.
History of InfraGard

- Immediate success moved program responsibility to FBI HQ under the Bureau’s Cyber Division, expanding the program to all 56 field offices, 400 satellite offices with 11,400 special agents
- In 2003, private sector members created the InfraGard National Members Alliance (INMA)
  - Formalized the private sector
  - Local IMA’s and the INMA are 501(c)3 non-profit corporations with a Board of Directors
About InfraGard

- Each one of the **86 Chapters** across the US and its Territories is geographically linked with an FBI Field Office.
- Membership provides stakeholders access to over 28,000 experts from law enforcement, industry, academic institutions and other federal, state and local government agencies.
- Members are the owners and operators of the critical infrastructures in the community
Infragard Structure – National/Local

- INMA
- FBI HQ PPAU
- INFRAGARD MEMBERS
- LOCAL FIELD OFFICE
- Vetting

Approval process

86 IMA
56 LOCAL FIELD OFFICE
27,000+ INFRAGARD MEMBERS
**Critical Infrastructure Sectors (17)**

**InfraGard Membership (27,000+)**

**InfraGard Web Site (LSU)**

**Special Interest Groups (3)**

**chapter pages**

**local InfraGard chapters (86)**

**SIG pages**

**Chemical, Food/Agriculture, Research & Technology**

**member vetting**

**Coordination Intelligence links**
Infragard Membership

• Critical Infrastructure Owners/Operators
  ✓ Private Sector
  ✓ Public Sector

• Strategic Partners
  ✓ Local, State and Federal Law Enforcement
  ✓ Government Agencies (DHS)
  ✓ Other First Responders

• Trust Relationship
  ✓ All members have FBI Security Clearance for Law Enforcement Sensitive information
Involvement: Private Sector and Local Governments

- Corporate Risk Management Department
- Executive Management / Board of Directors
- IT Department
- Security Department
- Human Resources Department
- Operations staff
- Other responsible individuals
Membership in InfraGard is granted by the FBI. However, InfraGard Membership is maintained at the local Members Alliance level.

- Select which of the 86 chapters to affiliate with.
- Submit application to the local FBI InfraGard Coordinator or the IMA Membership Coordinator.
- All applicants undergo a records check performed by the FBI.
- No cost to join InfraGard.
- Go to www.infragard.org or www.wi-infragard.com to join or for more information.
Infragard National Initiatives

Current structure provides program flexibility beyond the FBI. The INMA currently has MOU’s in place with:

- FBI
- DHS
- ATF
- BENS (Business Executives for National Security)

- iKeepSafe Coalition (outreach to schools/families for Internet safety)
- GETS/WPS Card Program
- TSA Registered Traveler Program
- igc.infragard.org secure website
- CyberCop Portal (shared with other law enforcement entities)
- “The Guardian” – periodic enewsletter
Critical Infrastructure Sectors

- Banking & Finance
- Chemical & Hazmat
- Public Health
- Emergency Services
- Food & Agriculture
- Education
- Postal & Shipping Transportation
- Information Technology
- Telecommunications
- Commercial Properties
- Government Facilities
- Defense Contractors
- National Monuments
- Energy
- Manufacturing
- Water
- Wastewater, Dams
- Nuclear
Office of Homeland Security
Critical Infrastructure Protection Program

- Indicators of Potential Terrorist Activity
- Understanding the Threat
- Public and Private Sector Partnerships
- Information Sharing
- Pre-Incident and Emergency Planning
- Suggested Protective Measures
Critical Infrastructure Protection

- Terrorist activity does not occur in a vacuum
- Planning /Preparation provides opportunity for detection
- Community members are in the best position to observe these early warning indicators
- Pre-Incident indicators can be scouting, weapons acquisition, or vehicle rentals
Critical Infrastructure Protection

- Specialized knowledge possessed by industry practitioners is an invaluable resource for Law Enforcement
- Preventing terrorism is a community effort
- Success can come from effective partnerships between the community and law enforcement
Example: water Sector
<table>
<thead>
<tr>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dover Force Protection - February 18-25</td>
<td>02/25/10</td>
</tr>
<tr>
<td>Purported Radioactive Material Canister Likely Counterfeit</td>
<td>02/25/10</td>
</tr>
<tr>
<td>The CIP Report - Volume 8 Number 8</td>
<td>02/23/10</td>
</tr>
<tr>
<td>2010 Vancouver Olympics and Paralympics: Little Health Threat to the</td>
<td>02/22/10</td>
</tr>
<tr>
<td>United States</td>
<td></td>
</tr>
<tr>
<td>Identification of 174 Encrypted Internet Protocol Addresses Used in</td>
<td>02/22/10</td>
</tr>
<tr>
<td>Waledac Malware Attacks, as of September 2009</td>
<td></td>
</tr>
<tr>
<td>Compromise Of US Business Computer To Host A Phishing Scheme That</td>
<td>02/22/10</td>
</tr>
<tr>
<td>Spoofer An Identified Online Payment System, With Connections To</td>
<td></td>
</tr>
<tr>
<td>Russia, Singapore, And Other Countries</td>
<td></td>
</tr>
<tr>
<td>Austin Plane Crash a Deliberate Act</td>
<td>02/19/10</td>
</tr>
<tr>
<td>High-Profile Events Hosted in the United States and Canada in 2010</td>
<td>02/18/10</td>
</tr>
<tr>
<td>Present Potential Targets for Violent Anarchist Extremists</td>
<td></td>
</tr>
<tr>
<td>Cyanide - Easily Obtainable Chemical of Interest to Terrorists</td>
<td>02/18/10</td>
</tr>
<tr>
<td>The Terrorist Threat to Cross-border Electricity Infrastructure in</td>
<td>02/17/10</td>
</tr>
<tr>
<td>Washington State and British Columbia, Canada</td>
<td></td>
</tr>
</tbody>
</table>
Western Wisconsin Infragard Sectors
Locally relevant but follow NIPP

- Banking & Finance
- Tourism & Public Venues
- Chemical & HazMat
- Defense Industrial Base
- Education
- Emergency Services (LE, Fire, EMS, EM)
- Health Care (PH, Hospitals)
- BioTech
- Research & Technology
- Food & Agriculture
- Government (+ Border/POE’s)
- Information Technology
- Telecommunications
- Transportation (Air/Sea/Ground/Pipelines)
- Water/Wastewater (+ Dams)
- Energy
- Nuclear Power
Infragard Activities

- Strategic Planning
- Quarterly Membership Meetings
  - Information exchange/training/recruiting
- Periodic Sector Chief Meetings
  - Coordinate sector operations
  - Support local/regional Fusion Centers (they don’t support us)
- Local outreach
- Special events & exercises
- Meetings attended by
  - Local InfraGard members (from industry, academia, public sector)
  - Local FBI field office (SAC, ASAC, SSAs, SAs)
  - DHS Protective Security Advisors (PSA)
  - Other federal/state/local agencies
Open Source, FOUO & LES

• Information Disseminated to members
• DHS Daily Reports
• FBI Threat & Intelligence Bulletins
• Regional Terrorism Threat Assessment Center (RTTAC)
• Joint Terrorism Task Force (JTTF)
• LECC (Law Enforcement Coordination Center)
• Infragard Secure VPN (LSU-hosted)
Participation in Special Interest Groups (SIGs) requires both:

- Membership in InfraGard, and
- Affiliation with the respective industry (i.e., Chemical industry for ChemGard)

SIG members:

- Have access to secure areas of the FBI’s Clientless VPN dedicated to the respective SIG
- May submit articles & information on sector-specific protection topics to be posted on the SIG area of the VPN
- May communicate about sector-specific issues via message boards in a secure environment
**AgGard**
- Connects members from agriculture community with scientists, state and local LE, and the FBI regarding suspicious or unusual activity – works with FBI’s WMD Directorate under NS Branch

**ChemGard**
- Private sector stakeholders partner with government to assist in detecting, deterring, assessing and preventing threats & attacks targeting the chemical sector
- Collaborative effort between the Counterterrorism and Cyber Divisions of the FBI

**Research & Technology Protection (RTP) SIG**
- Dedicated to the safeguarding of new & developing technologies from illegal acquisition by foreign adversaries
- Partnership with the Defense Research & Acquisition Community and Service Counterintelligence Support Agencies (NCIS, OSI, Army 902d MIG, etc.)
- Monitored by the FBI’s CI-Domain Section
Benefits to CI/KR Sector

- Access to locally-relevant security training
- Networking venue for all agencies in region
- Access to threat information
  - Briefings
  - On-line
- Knowledge of other CI/KR in local region
- Access to subject matter experts across all sectors
Infragard and DHS Coordination

- Infragard is local/regional in scope but covers all CI/KR sectors in the region.
- DHS Information Sharing & Analysis Centers (ISAC’s) are national in scope and cover one sector.
Infragard and Fusion Centers

Infragard

RTTAC

Terrorism

JTTF (FBI Lead)

Terrorism

LECC

All-Crimes

Deconfliction

Watch Center

Local FBI

Infragard

TEWG

TLO Program

CI/KR Program

Local P/S

County OEM

Private Sector

Local Govts

Local Public Safety

NIN

Gangs

Border Crimes

Violent Crimes

Private Sector

Local Govts

Local Public Safety

FBI

Local P/S

County OEM

OEM
Ex: Transportation Sector

- Highway Watch (commercial vehicles)
- School Bus Watch (school transportation providers)
- Surface Transportation (rail systems)
- Public transportation (subset of ST ISAC – mass transit systems)
- Maritime
MOU’s

- ISSA – complete
- ASIS – close to completion
- AWWA (Includes wastewater)
- WEF
- Rural Water
- Others such as WDBC (Water Design Build Council as an example)
How ISAC’s Work (Highway Watch)

- Highway Watch Call Center (ATA)
- Highway ISAC (TSOC)
- Homeland Security Information Network (HSIN) and other Intel networks

all highway users
InfraGard Community Outreach Programs

- Education on what qualifies as suspicious behavior and how to report it to those in and out of our communities
- State-Wide reporting location
- Leverage service workers and technicians
- Community Watch & Real Estate Groups
- Workplace Security Training
- Community Watch Program
InfraGard Community Outreach Program

- Service Groups
  - Utility Meter Readers
  - Cable TV Technicians
  - Telecommunications Technicians
  - Postal Workers
  - Waste and water/wastewater Engineers
  - Security Technicians
  - Emergency Services Members
InfraGard Community Outreach Program

- Community & Real Estate Groups
  - Neighborhood Watch
  - Community Organizations
  - Realty Groups
  - Property Management Groups
  - Kiwanis
  - Rotary Club
Water ISAC

Water/Wastewater Security Network

www.WaterISAC.org

www.waterisac.org
ISACs

- WaterISAC is one of several ISACs

- Information Sharing & Analysis Centers

- Facilitate information sharing to protect infrastructure and recover from security incidents and natural disasters.
Failure is not an option.

- There is no excuse for not being informed and prepared for natural disasters and security threats.

- Mission: To be a one-stop, authoritative source for essential information on infrastructure protection.
About WaterISAC

- Developed at the urging of U.S. EPA and the FBI’s National Infrastructure Protection Center.

- Authorized by Congress.

- Established in 2002 as a not-for-profit organization, governed by board of utility managers and state administrators.

- Includes wastewater and dams
Background

- Information Sharing and Analysis Centers – per Presidential directives in the 1990s - facilitate the exchange of threat information between the federal and private sectors
- Authorized under the Bioterrorism Act
- Launched in 2002 by utility managers as a non-profit
- Designated the official communications/operations arm of the Water Sector Coordinating Council
- 10,000 Basic subscribers; 1,500 Pro subscribers (projected growth to 15,000 by end of 2010); 95% utility staff
Information for Decision Making

- The only centralized, real-time source for security and emergency management information

- Information that utilities need to make strategic and operational decisions for:
  - Risk evaluation
  - Capital investment and operational planning
  - Preparation for potential security incidents and disasters
# WaterISAC: Two Levels of Service

<table>
<thead>
<tr>
<th>Basic</th>
<th>Pro</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Basic information</td>
<td>✓ Comprehensive, one-stop shop</td>
</tr>
<tr>
<td>✓ Public-release EPA or DHS documents</td>
<td>✓ Sensitive, limited distribution information</td>
</tr>
<tr>
<td>✓ Free</td>
<td>✓ Private, public sources</td>
</tr>
<tr>
<td></td>
<td>✓ Free webinars on hot topics</td>
</tr>
<tr>
<td></td>
<td>✓ Access to analysts 24/7</td>
</tr>
<tr>
<td></td>
<td>✓ Collaboration tools</td>
</tr>
<tr>
<td></td>
<td>✓ Annual fee (except for trial)</td>
</tr>
</tbody>
</table>
WaterISAC Pro Services

- Searchable library of more than 2,000 papers and reports, guidance documents and best-practices
- Peer-to-peer online collaboration and sharing
- Vulnerability assessment tools
- Contaminant databases
- 24/7 access to homeland security analysts
- Threat alerts
Who Subscribes

- U.S., Canadian and Australian—
  - Utility staff: GMs, security, water/wastewater quality, IT
  - State and federal agencies: water/wastewater quality, water/wastewater resources, homeland security, emergency response, intelligence, law enforcement
  - Circuit riders
  - State water/wastewater associations
Sources of Information

- Private and proprietary sources
- Federal and state/provincial government agencies
- Utilities and utility associations
- Media and other open sources
- Collected by intelligence analysts
Information Protection

- Need-to-know access (applicants are vetted)
- Two-factor authentication to access Pro portal
  - Via token or cell phone app
- Restricted dissemination of information
Webinars for Pro Subscribers

- Recent
  - Lessons Learned From Hurricane Katrina
  - Water/Wastewater/wastewater Agency Response Networks
  - Insider Threats
  - H1N1 Update w/ CDC
  - Using Social Media to Communicate With Consumers

- Planned
  - Current Terrorism Threats
  - Incident Management Training

Take a Tour
- Every other Thursday
Collaboration & Networking

- Exclusive, secure collaboration spaces for working groups
  - Draft, edit and share documents online
  - Solicit comments
  - Send secure e-mail
  - Not just for collaboration on sensitive security issues

- Share knowledge and experience with colleagues
  - Participate in online discussions or start your own
McAfee Report on Control System Security

This report, published by the security firm McAfee, reveals the extent to which the economic downturn is set to impact the security of vital information. Information is becoming firmly established as an international form of currency, and cyber-criminals are increasingly targeting businesses for profit. The sources of threats are shifting, and new nations are emerging as perceived threats to data security. The report concludes with suggested best practices for protecting valuable digital assets.

While this report was written mostly for for-profit businesses, utilities face many of the same threats and can benefit from the same best practice suggestions.

McAfee Cyber Report.pdf (7.0 MB)
View Download

Tags: scada, cyber threat, cyber insider, insider threat

There are no comments on this document
## Tools And Applications

<table>
<thead>
<tr>
<th>Tools And Applications</th>
<th>Discussions</th>
<th>Documents</th>
<th>Blog Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Training and Exercises</td>
<td>0</td>
<td>87</td>
<td></td>
</tr>
<tr>
<td>Training Aids</td>
<td>0</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>VSAT</td>
<td>0</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Blast Vulnerability Tool</td>
<td>0</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>SewerNet</td>
<td>0</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>PipelineNet RiverSpill</td>
<td>0</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Chlorine Gas Decision Tool</td>
<td>0</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Water Distribution System Decision Tool</td>
<td>0</td>
<td>2</td>
<td></td>
</tr>
</tbody>
</table>

**Actions**
- Start a discussion

**Notifications**
- Receive email notifications
- View feeds

**Download External Tools**
- WISER
Utilizing Twitter for Support System Announcements

Are any of the WaterISAC members using Twitter [http://www.twitter.com](http://www.twitter.com) or [http://www.twitter.com/LIS](http://www.twitter.com/LIS) or one of its clones to notify customers/special populations about water quality exceedences or other public health situations? If so, has it been successful - and how do you track success?

---

1. Feb 25, 2009 1:07 PM in response to Allan Tarket

Re: Utilizing Twitter for Support System Announcements

Hello Allan,

We've "just" set up a Twitter account for our company ([http://twitter.com/wawnc](http://twitter.com/wawnc)) and are about to begin a test program to see what sort of information is best to disseminate through that account.

At this point, while all the Internet's aTwitter about the service, it is nowhere near a saturation point: a recent Pew Internet Report states that:

"As of December 2008, 11% of online American adults said they used a service like Twitter or another service that allowed them to share updates about themselves or to see the updates of others.

Twitter and similar services have been most avidly embraced by young adults. Nearly one in five (19%) online adults ages 18 and 24 have ever used Twitter and its ilk, as have 20% of online adults 25 to 34. Use of these services drops off steadily after age 35 with 10% of 35 to 44 year olds and 5% of 45 to 54 year olds using Twitter. The decline is even more stark among older internet users; 4% of 55-64 year olds and 2% of those 65 and older use Twitter."

So, at best - 11% are using some sort of service, not necessarily Twitter, so we may need to take all of them into account (Plurk, Jaiku, Facebook, Friendfeed et al.) On my personal account, I use Ping.fm to send one message that then gets propagated to accounts at all of these.

Also, while it was originally used primarily as an SMS service (thus the 140 character limitation), I would venture a guess that the vast majority of people now use Twitter via software clients that may or may not receive messages immediately.

As a part of a larger notification program I see it is a no-lose situation.

But without some sort of service-level agreement or direct, immediate method to determine its effectiveness at reaching a certain populace I think it is going to take early adopters willing to make mistakes to help us gauge its worth or usefulness as a notification tool when it comes to something as important as water / health / safety information.

(Aside: Lenny Zeltser wrote a good article on various ways to work with Twitter in [How to Use Twitter for Information Mining](http://www.lenm.com/twitter/) for people looking to get a feel for how it is being used.)

My particular expertise is in information security and there is a fairly large contingent of people in that realm on Twitter, making it a great resource for me.

I'm also on the Board of the [NY Metro InfraGard](http://www.nymetroinfragard.org), an FBI Program for information sharing regarding critical infrastructure protection. As a distributed organization of more than 28,000 CIIP professionals, I see Twitter becoming a useful and fast method for info sharing. My pet project right now is to find the best grouping of social tools to help in this regard, and I've been in contact with some folks working on similar projects for DoD and DHS.

So, after all that I'm sorry I don't have any hard data to share at this point - but I'm working on it and hopefully something I've mentioned will be useful. I'd certainly like to hear what others' experiences are as well.

Regards,

John Tierney, CISSP CISA NSA-IAM/IEM

[http://twitter.com/jjt](http://twitter.com/jjt)
**ER CIPAC Meeting Calendar (all times listed in Eastern)**

<table>
<thead>
<tr>
<th></th>
<th>Sunday</th>
<th>Monday</th>
<th>Tuesday</th>
<th>Wednesday</th>
<th>Oct 1</th>
<th>Thursday</th>
<th>Friday</th>
<th>Saturday</th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>September 24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td></td>
<td>September 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td></td>
<td></td>
<td>September 23</td>
<td></td>
<td></td>
<td>October 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td></td>
<td></td>
<td></td>
<td>November 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>26</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>29</td>
<td></td>
<td></td>
<td>September 24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>31</td>
<td></td>
<td></td>
<td>September 30</td>
<td></td>
<td></td>
<td>October 31</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Recent Content**
- ER CIPAC Sixth Conference Call Agenda – October 23
- Draft Priorities Document
- All-Hazard CMP Document (for Council Review)
- Re: High Priority: Exercise Emergency Response Plans
- Re: Top Priority: Update Emergency Response Plans
- Re: Other Project Ideas
- Re: Fort Worth Water Treatment Plant Tour
- High Priority: Develop Emergency Communication Lessons Learned – Ideas 3 – 6 (of 6)
- Georgia WARN ERP Example
- Priority Activities: Raise Awareness of Interdependencies
- Priority Activities: Update Vulnerability Assessments at Regular Intervals
- Priority Activities: Update Mutual Aid Agreements

**Upload and Edit Documents**
- Start a discussion
- Create a document
- Create an announcement
- Create a poll

**Notifications**
- Receive email notifications
- View feeds
Wastewater Resources on WaterISAC

✓ Suite of Water Environment Research Foundation (WERF) Reports and Tools:


✓ Software to Prioritize Wastewater Asset Failure and Security Risks

✓ Strategies for Small Wastewater Systems for Risk Reduction and Safeguarding Assets

✓ Chemical, Biological, and Radiological Sensors for Early Warning Systems in Wastewater Utilities
Wastewater Resources on WaterISAC

- SewerNet: Integrated, GIS-based Consequence Assessment Model for Sewer and Storm water
- DHS Protective Security Division Paper: “Characteristics and Common Vulnerabilities Infrastructure Category: Community Wastewater Treatment Facilities”
Wastewater Resources on WaterISAC

- WaterISAC’s Unique Social Networking Features Designed to Increase Horizontal Communications Between Wastewater Utility Owner/Operators
Sign Up for FREE Access

- In partnership with U.S. EPA
- 12 months of FREE access, for—
  - Drinking water/wastewater and wastewater/wastewater utility staff
  - State and federal government agency staff
  - Circuit riders
  - State water/wastewater/wastewater utility association staff
- E-mail: Sign up at www.waterisac.org
Capabilities/Services

- Threat alerts by e-mail and, if necessary, by phone
- Chem/bio databases
- 2000+ papers, bulletins, guidance docs, etc.
  - Emergency management
  - Security threats
  - Training
  - Vulnerability assessment tools
Capabilities/Services

- Web 2.0: The Power of Social Networking
  - Send secure e-mail
  - Search online directory
  - Participate in online discussions
  - Share knowledge and experience with colleagues
  - Create exclusive, interactive working groups for collaborating on projects
In Conclusion ...

✓ Do you already subscribe to one or the other programs? Login and participate! Your colleagues are waiting!

✓ Not yet a subscriber?

✓ Take advantage of the trial at water/wastewater ISAC!

✓ Contact Aaron Levy: levy@waterisac.org at www.waterisac.org

✓ Subscribe at Infragard.net
QUESTIONS?

For more information:

Norman Arendt, PhD
Safety Director SEH
President Infragard Madison members Alliance

njarendt@tds.net
narendt@sehinc.com
608.345.1412

Thank You for Your
Interest in Infragard and
the water/wastewater
ISAC!
Contact Numbers

- Wisconsin Statewide Information Center
  - 608-240-3592
  - [http://www.wilenet.org/](http://www.wilenet.org/) (LE Only)

- FBI Joint Terrorism Task Force
  - Madison 608-833-4600
  - Milwaukee 414-276-4684

- National Terrorist Screening Center
  - Washington DC 866-872-9001

- Local Law Enforcement
Additional Slides
A Call to Serve

- Be Vigilant
- Report suspicious activity
- Practice best security procedures
- Make a difference in your community!
Seven Signs of Terrorism

- Surveillance
- Elicitation
- Tests of Security
- Acquiring Supplies
- Suspicious person out of place
- Trial Run / Dry Run
- Deploying Assets
What is suspicious activity?

- Pictures being taken at odd hours
- Pattern of False Alarms requiring a response by Law Enforcement or Emergency Services
- Recent damage to a perimeter fence or gate
- Unfamiliar cleaning crews or contract workers
- Unusual maintenance activities
- Persons parking or loitering in the same area over a multiple day period with no apparent reason
Pre-Attack Indicators

- Persons with maps or facility photos, notes regarding infrastructure or personnel lists
- Persons may be carrying luggage or backpack
- Persons that appear to be focused and vigilant
- Displays nervousness and profuse perspiration
- Makes attempt to blend in with crowd
- Walking with deliberation or running in a suspicious manner
Workplace Security

- Social Engineering
- Theft of contractor ID’s, facility ID / Access cards or uniforms
- Requests for odd hours or assignments
- Wanting detailed information about client locations not usually needed
- Signs of stress or agitation
- Problems with co-workers, management
Surveillance Facts

- Thieves case neighborhoods, walk around the block, sit in cars
- Observes neighborhood activity, detects patterns of behavior
- May pose as housekeeper, lawn maintenance, survey taker or salesman
- Asking questions about vacant homes, or neighbors work routines
Surveillance Facts

- Insider knowledge, employee threat
- Patience, planning can take months
- Detailed escape / contingency plans
- Looking for routines and consistency and patterns in operations

The observation of any ONE INDICATOR may NOT, by itself, suggest terrorist activity, however, each should be considered along with all other relevant observations.
Why haven’t we seen more attacks in the USA

- US Citizens have been vigilant and report suspicious persons & activities
- Enhanced investigative authority and power of Federal, State and Local Law Enforcement Departments
- Increased funds & resources to vigorously predict, prevent, and / or counter a terrorist attack or the impact of such an attack
Roadmap to Security

- Greatest Vulnerabilities
  - Complacency, Failure to Plan, Exercise, Train & Improve Together

- Greatest Deterrents
  - Vigilance, Communications, Teamwork, Disruptive Environment

- Use of State & Federal Funds Wisely
Our Greatest Advantage

Common Focus & Unity of Effort

Terrorist groups within the US recognizing such effectiveness of action and coordination by the US, may feel impaired and have been unable to identify, plan and execute a successful attack.
Be On the Look Out

No one knows your environment better than you. You may see or hear things that seem out of the ordinary and may indicate illegal conduct.

- Immediately report people who do not have a legitimate reason to:
  - Photograph, Videotape or Sketch
  - Sit in cars for prolonged periods of time in a neighborhood or business district
  - Ask detailed questions
  - Seek blueprints of buildings and facilities
Use the **SCAN** Method when you:

- **See**: Suspicious or unusual activity and behaviors
- **Confirm**: Memorize physical features, vehicle description & license plate, details of incident, location / time. Write it down when safe.
- **Ask**: If approached, be polite and assess reaction, do not be confrontational
- **Notify**: Immediately notify authorities in your area or contact the FBI or DMA Duty Officer

www.homelandsecurity.wi.gov
24-Hour Duty Officer 1-800-943-0003
608-242-3232
Information to Record

- **Suspect Information**
  - Sex, Race, Age, Height/Weight, Hair/Eye Color

- **Clothing**
  - Shirt, Pants, Shoes, Hat, Glasses, etc.

- **Identifying Features**
  - Scars, Hair, Tattoos, Speech, other

- **Vehicle Information**
  - Make/Model, Year/Color, License Number, Damage, Direction of Travel