CYBERSECURITY THREATS TO THE WATER SECTOR

Jason Burt
Cybersecurity Advisor, Region IV
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency

Divisions of CISA

- CISA consists of:

Cybersecurity Division

Infrastructure Security Division

Emergency Communications Division

National Risk Management Center

CISA Mission and Vision

Cybersecurity and Infrastructure Security Agency (CISA)

Mission:

- Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

Vision:

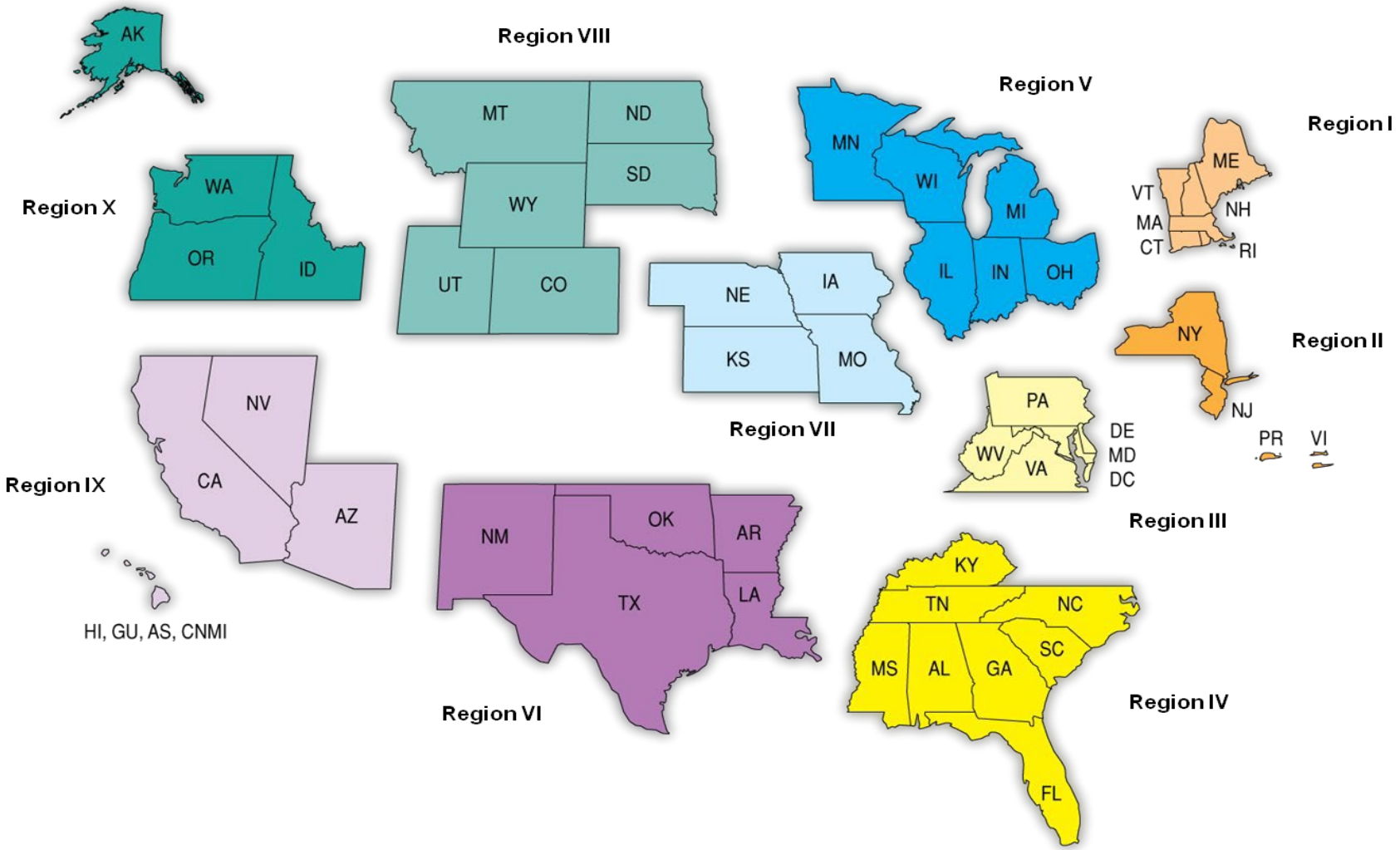
- A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive

Jason Burt
March 5, 2021

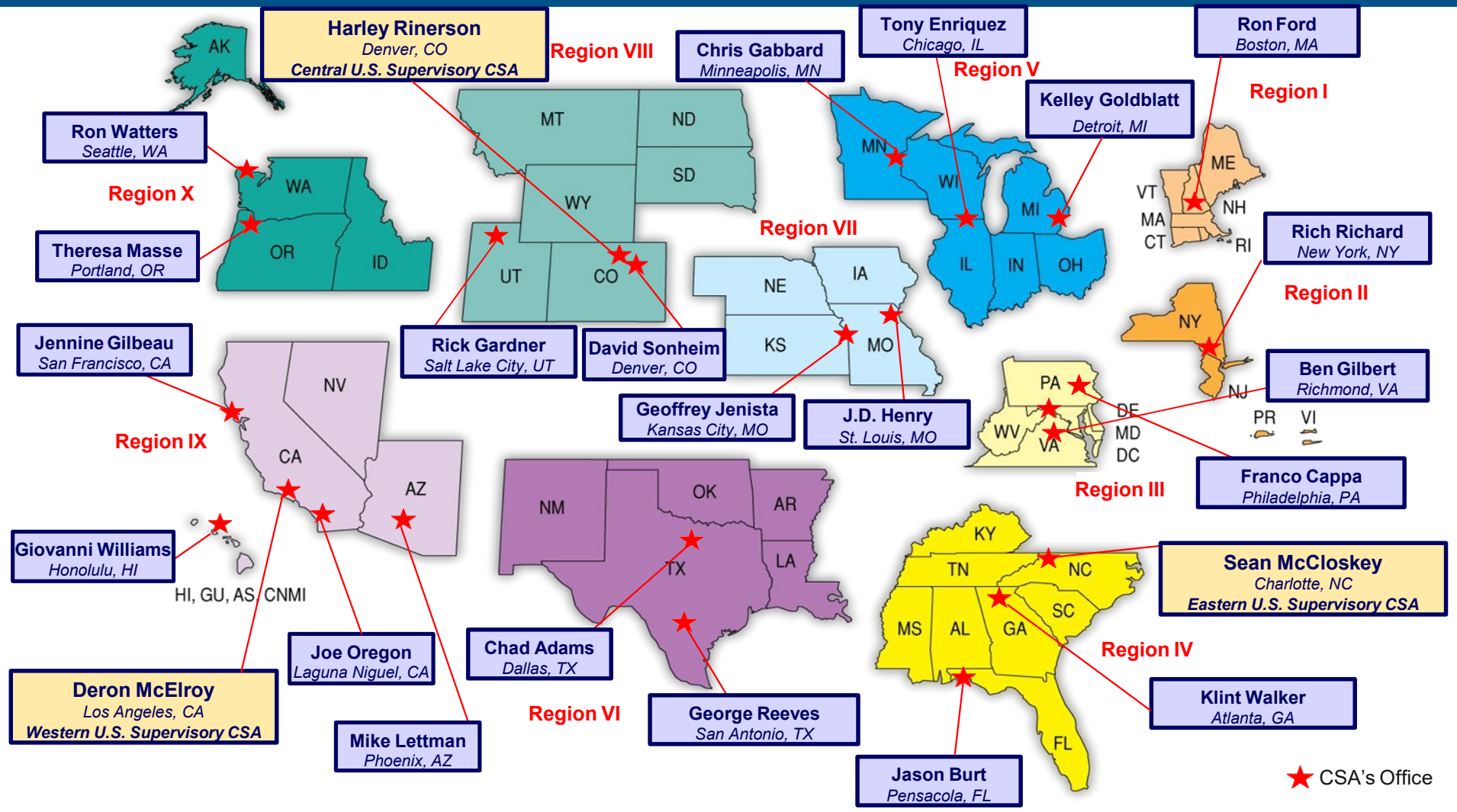
CYBERSECURITY ADVISOR PROGRAM

Jason Burt
March 5, 2021

CSA Deployed Personnel



CSA Deployed Personnel



Serving Critical Infrastructure

Jason Burt
March 5, 2021

CYBER THREATS TO WATER

U.S. WATER UTILITY

Event: January 2011, U.S. water utility reports a security breach of its remote terminal service machine that allows access to the SCADA system

Impact: Remote logon service for after hours access was not responding, but no impacts to the SCADA network were observed

Specifics: 7,463 incidents of malware traffic were communicating with the utility's computers. Only 77 were unique known malware (spam, bruteforce ssh, virus/worms) originating from 57 compromised hosts. Analysis concluded that the observed activity was crimeware related.

Lessons learned:

- Secure remote access with solutions such as VPN or two-factor authentication
- Leverage the static nature of a control system to look for anomalies
- Prepare and utilize an incident response plan

HARRISBURG PENNSYLVANIA WATER SYSTEM

Event: Foreign hacker penetrated security at a water filtering plant

Impact: The intruder planted malicious software that was capable of affecting the plant's water treatment operations

Specifics: The infection occurred through the Internet and did not seem to be an attack that directly targeted the control system

Lessons learned:

- Secure remote computers
- Defense-in-depth strategies, firewalls and intrusion detection systems
- Critical patches and antivirus needs to be applied and updated regularly

MAROOCHY WASTE WATER

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station

Lessons learned:

- Suspend all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions

Jason Burt
March 5, 2021

ICS “NON-INCIDENT” - WATER

- **Event:** November 2011, FOUO report detailing a suspected water district cyber intrusion was publicly disclosed.
- **Impact:** Media spin on this “attack” caused bad publicity for the utility and led to wasted time and effort by those trying to mitigate the issue.
- **Specifics:** Discovery of Russian IP addresses led to an assumption that this was a cyber attack by an outside source. However, the Incident Response Team analysis disproved this theory and determined it to be a physical failure of the pump over a period of time.

Lessons learned:

- Handle sensitive materials according to the designated label (do not publicly disclose FOUO materials).
- Perform regular maintenance.

WATER UTILITY LOSES CONTROL

Event: Residents of a rural town experienced loss of water pressure.

Impact: Approximately 10,000 residents were without water.

Specifics: Utility operator updated its HMI OS (Windows) with a direct connection to the Internet and evidence points to a virus infecting the SCADA system; causing it to crash.

The ICS was outdated, not supported by the vendor, and not patched to current updates. It also lacked a firewall between the business and control networks.

Lessons learned:

- Utilize DMZ to ensure isolation from business side and Internet
- Keep systems patched
- Establish and enforce sound security policies

OLDSMAR WATER TREATMENT INCIDENT

Event: SCADA operator noticed remote access to control system.

Impact: Sodium Hydroxide level increased from 100 ppm to 11,100 ppm.

Specifics: Two separate incidents. Operator stated that TeamViewer was used to remotely access SCADA control system. Chemical level increased. Operator adjusted level back to normal value and disconnected the system from the network.

- HMI running Windows 7
- Multiple Remote Access programs running
- TeamViewer immediately uninstalled

Lessons learned:

- Never uninstall applications – Disconnect from NET and report.
- Limit Internet exposure to SCADA systems
- Segment Network
- Enforce Role-based Security & Logging

WATER-ISAC BEST PRACTICES

TOP 10 CYBERSECURITY BEST PRACTICES

1. Inventory Control System Devices & Restrict Exposure to External Networks
2. Implement Network Segmentation & Utilize Firewalls
3. Use Secure Remote Access Methods
4. Establish Role-based Access Controls & Implement System Logging
5. Implement a Strong Password Policy
6. Maintain Awareness of Vulnerabilities & Keep Systems Patched and Updated!
7. Develop and Enforce Policies on Mobile Devices & Removable Media
8. Implement an Employee Cybersecurity Training Program
9. Involve Executives in Cybersecurity
10. Develop Incident Response Plan & Exercise/Test the plan!

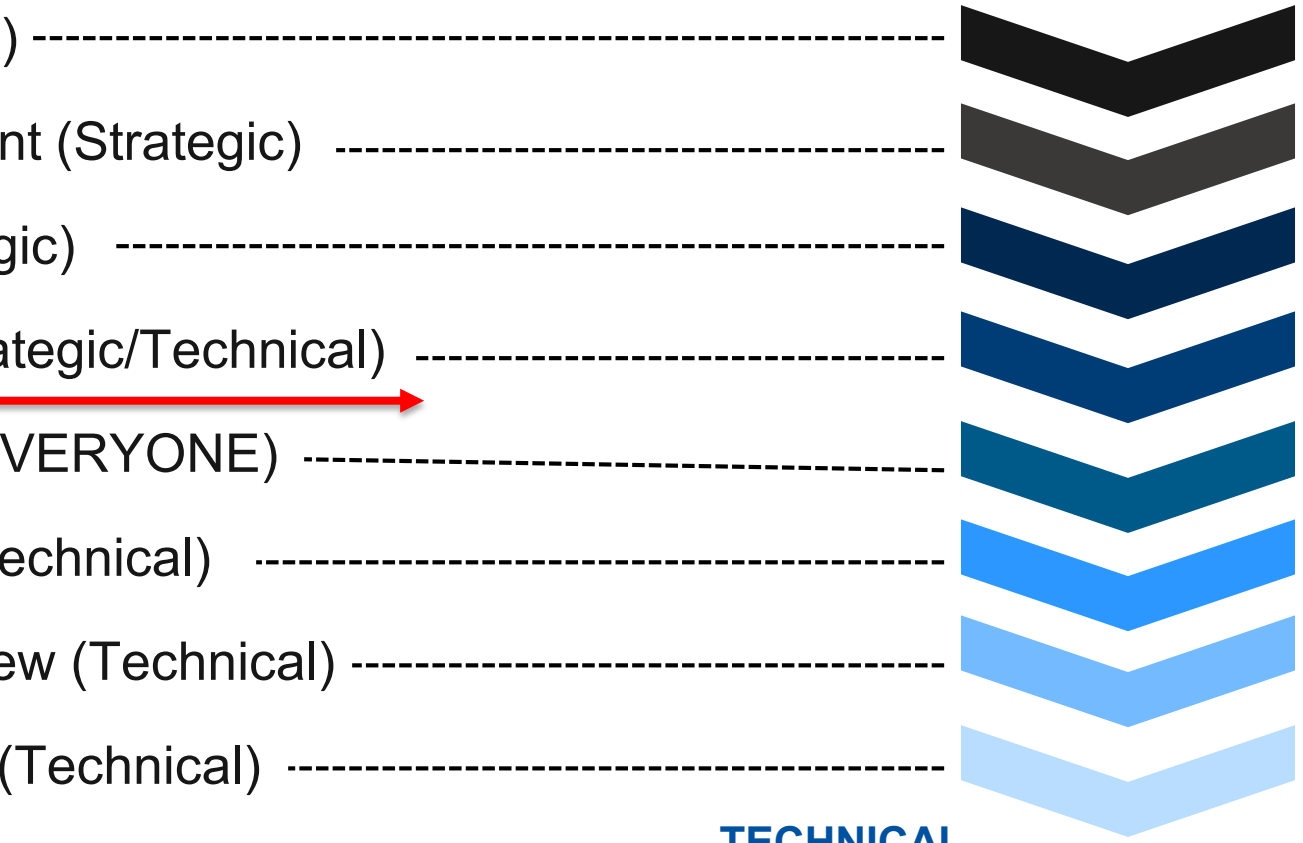
REPORT THE INCIDENT!

CISA CYBER SERVICES

Range of Cybersecurity Services

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)
- External Dependencies Management (Strategic)
- Cyber Infrastructure Survey (Strategic)
- Cybersecurity Evaluations Tool Strategic/Technical)
- Phishing Campaign Assessment (EVERYONE)
- Vulnerability Scanning / Hygiene (Technical)
- Validated Architecture Design Review (Technical)
- Risk and Vulnerability Assessment (Technical)



TECHNICAL
(Network-Administrator Level)

Jason Burt
March 5, 2021

Contact

CISA Contact Information

Jason Burt Region IV Cybersecurity Advisor (Florida, Alabama, Mississippi)	Jason.Burt@cisa.dhs.gov (202) 578-9954 (Cell)
Klint Walker Region IV Cybersecurity Advisor (Georgia, Tennessee, Kentucky)	Klint.Walker@hq.dhs.gov (404) 895-1127 (Cell)
Sean McCloskey Region IV Cybersecurity Advisor (North Carolina, South Carolina)	Sean.McCloskey@hq.dhs.gov (202) 578-8853 (Cell)