WaterISAC

The Water and Wastewater Systems Sector's Official Threat & Preparedness Resource

DHS Cybersecurity Advisor Program

| July 11, 2018 |

Today's Presenter

Tara Brewer, DHS CS&C

Slides and recording will be posted by Thursday.

DHS Cybersecurity Services For Water Sector

Tara Brewer
Cybersecurity Advisor
Stakeholder Risk Assessment and Mitigation
Office of Cybersecurity & Communications
National Protection and Programs Directorate

7/11/2018

Who We Are

Department of Homeland Security

National Protection and Programs Directorate

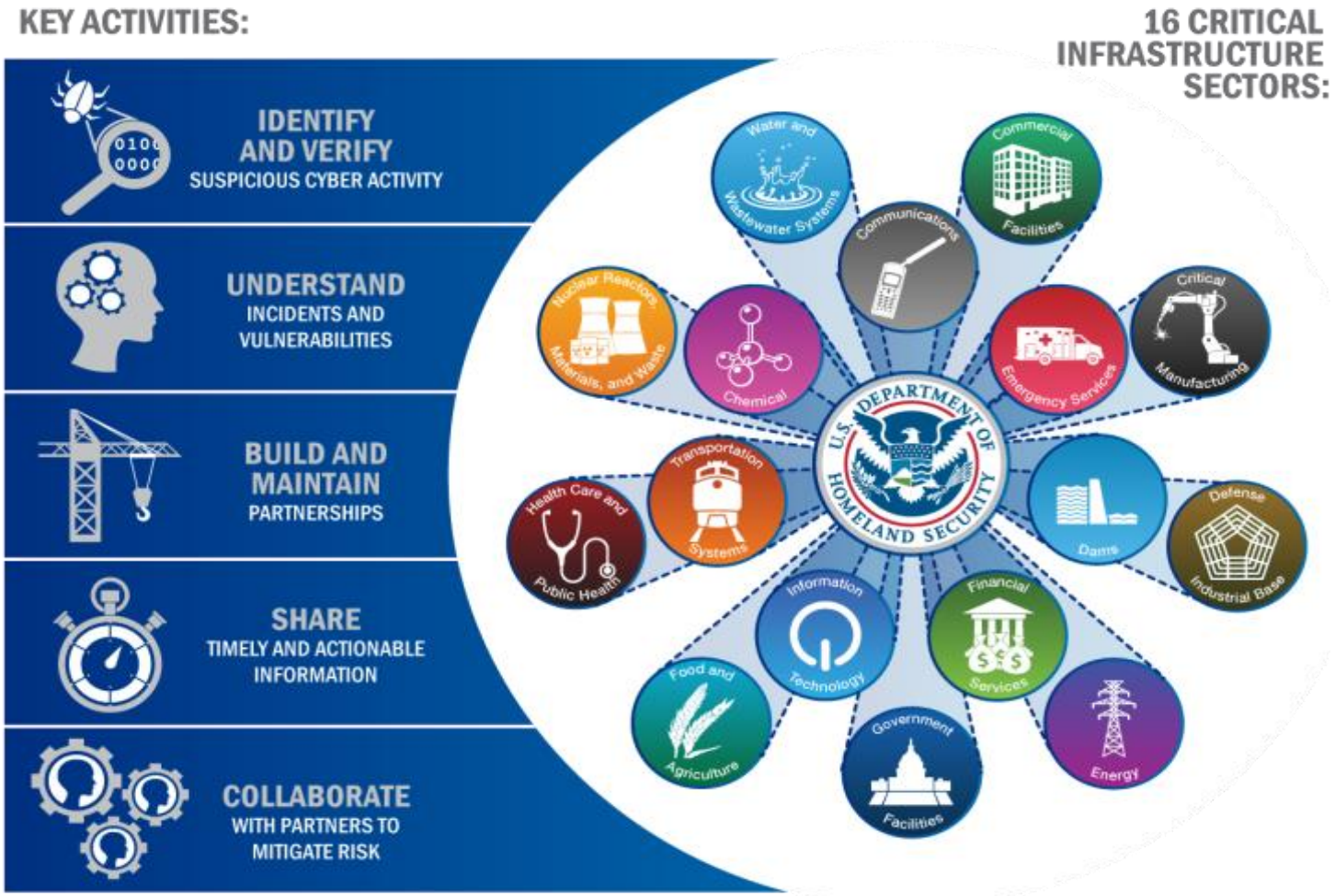
Office of Cybersecurity and Communications

- **Federal Network Resilience**
- **Network Security Deployment**
- **National Cybersecurity and Communications Integration Center**
- **Stakeholder Engagement and Cyber Infrastructure Resilience**
- **Office of Emergency Communication**

CS&C Mission:

Enhancing the security, resilience, and reliability of the Nation's cyber and communications infrastructure.

Serving Critical Infrastructure and SLTT Government



Cybersecurity Advisor (CSA) Program

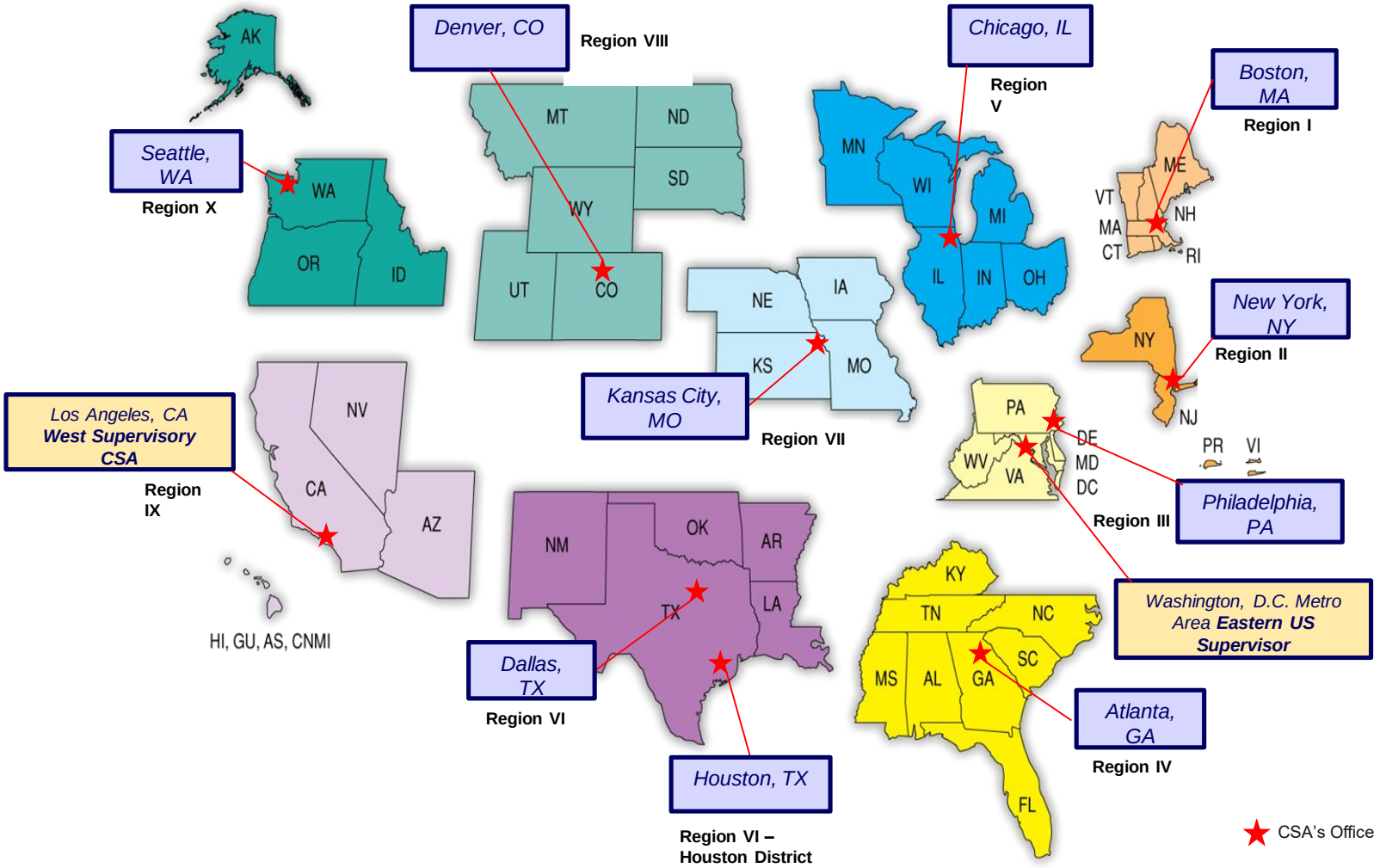
The CSA Mission:

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

In service of this mission, CSAs are guided by the following goals:

- **Assess**: Assess critical infrastructure cyber risk.
- **Promote**: Promote best practices and risk mitigation strategies.
- **Build**: Initiate, build capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Educate and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Coordinate incident support and lessons-learned.

Cybersecurity Advisor (CSA) Locations



For more information about the CSA Program, schedule a review or assessment, email cyberadvisor@hq.dhs.gov.

Homeland Security

DHS Cybersecurity Services Available to the Water Sector

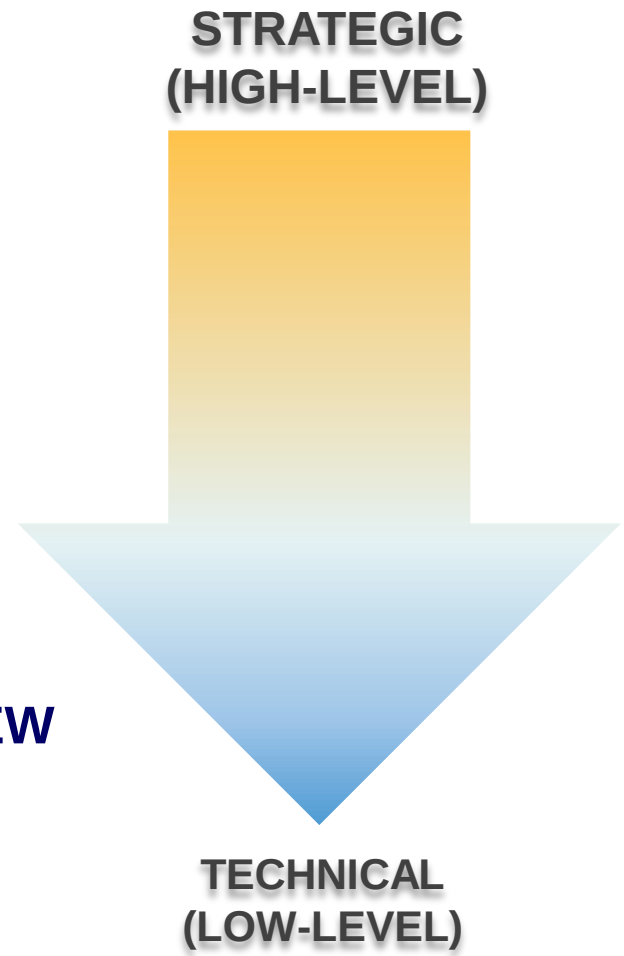
Cybersecurity Offerings

- National Cybersecurity and Communications Integration Center (NCCIC)
  - Operations
    - **US-CERT/ ICS-CERT Operations**
    - **Cyber Threat Hunting and Incident Response Teams**
    - **National Cyber Assessments and Technical Services (NCATS)**
      - **Risk and Vulnerability Assessments (RVAs)**
      - **Phishing Campaign Assessments (PCA)**
      - **Vulnerability Scanning**
      - **Validated Architecture Design Review (VADR)**
      - **Cyber Security Evaluation Tool (CSET™)**
  - Cyber Threat Detection and Analysis
    - **Cyber Exercises**
    - **Malware Analysis**
    - **National Cyber Awareness System**
    - **Publications and Communications**
- Stakeholder Engagement Cyber Infrastructure Resilience (SECIR)
  - Cyber Education and Awareness
    - **Federal Virtual Training Environment (Fed VTE)**
    - **National Initiative for Cybersecurity Careers and Studies (NICCS)**
    - **Stop.Think.Connect.™**
  - Partnership and Engagements
    - **State, Local, Tribal, and Territorial (SLTT) engagements**
    - **Critical Infrastructure Cyber Community Voluntary Program (C3VP) *http://us-cert.gov/ccubedvp***
  - Stakeholder Risk Assessment and Mitigations [a.k.a**. Cybersecurity Advisors**]
    - **Assessments**
      - **Cyber Resilience Reviews (CRR™)**
      - **External Dependency Management (EDM) Assessments**
      - **Cyber Infrastructure Surveys**
    - **Partnership Development**
    - **Stakeholder Preparedness**
    - **Incident Coordination**

Assessments

Cybersecurity Assessments

- CYBER RESILIENCE REVIEW
- EXTERNAL DEPENDENCIES MANAGEMENT
- CYBER INFRASTRUCTURE SURVEY
- CYBERSECURITY EVALUATIONS TOOL
- PHISHING CAMPAIGN ASSESSMENT
- VULNERABILITY SCANNING/ HYGIENE
- VALIDATED ARCHITECTURE DESIGN REVIEW
- RISK AND VULNERABILITY ASSESSMENT



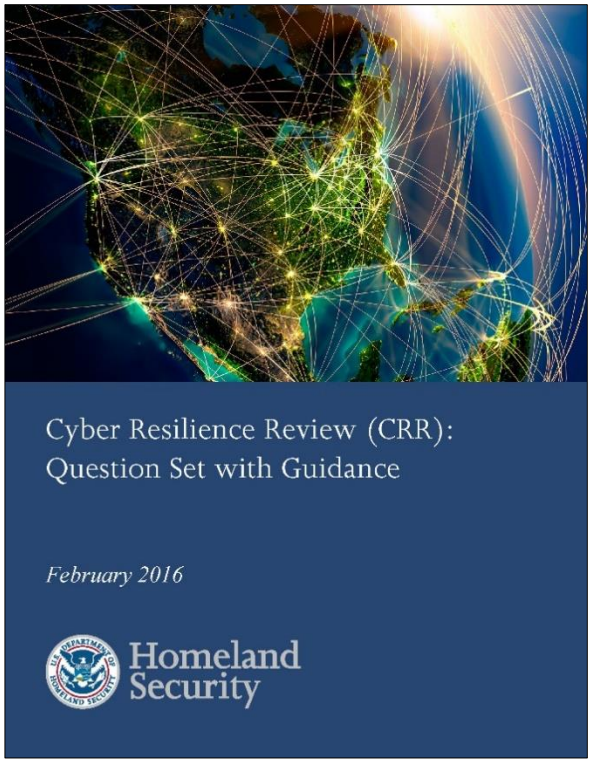
CYBER RESILIENCE REVIEW (CRR)

Cyber Resilience Review

- **Purpose:** The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its **critical services**
- **Delivery:** The CRR can be
  - **facilitated**
  - **self-administered**

  CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM))



CRR Question Set & Guidance

The CRR provides organizations with a no-cost method to assess their cybersecurity postures and measure against the NIST CSF.

Cyber Resilience Review Domains

Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know your biggest risks and address them in a manner that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable plans are in place to manage disruptions
Controls Management Manage and monitor controls to ensure they are meeting your objectives	**Situational Awareness** Actively discover and analyze information related to immediate operational stability and security
External Dependencies Management Know who your most important external entities are and manage the risks they pose to essential services	**Training and Awareness** Ensure your people are trained on and aware of cybersecurity risks and practices
Incident Management Be able to detect and respond to incidents	**Vulnerability Management** Know your vulnerabilities and manage those that pose the most risk

For more information: http://www.us-cert.gov/ccubedvp

Process Institutionalization

Maturity indicator levels (MIL) are used in the CRR to measure process institutionalization:

Processes are defined, measured, and governed

Practices are performed

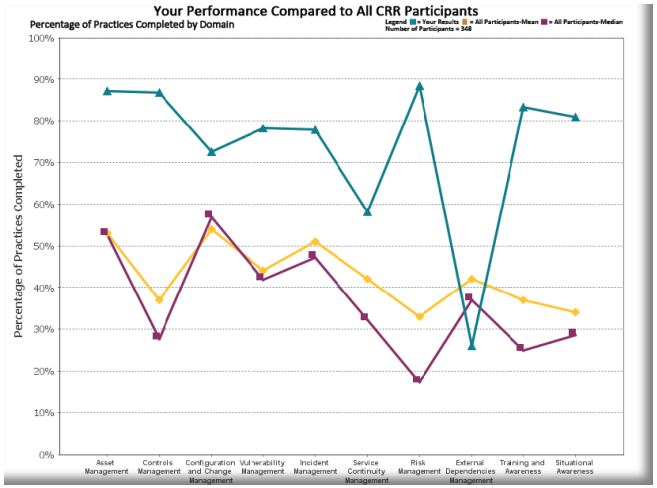
Practices are incomplete

Higher degrees of institutionalization translate to more stable processes that

- produce consistent results over time
- are retained during times of stress

CRR Sample Report

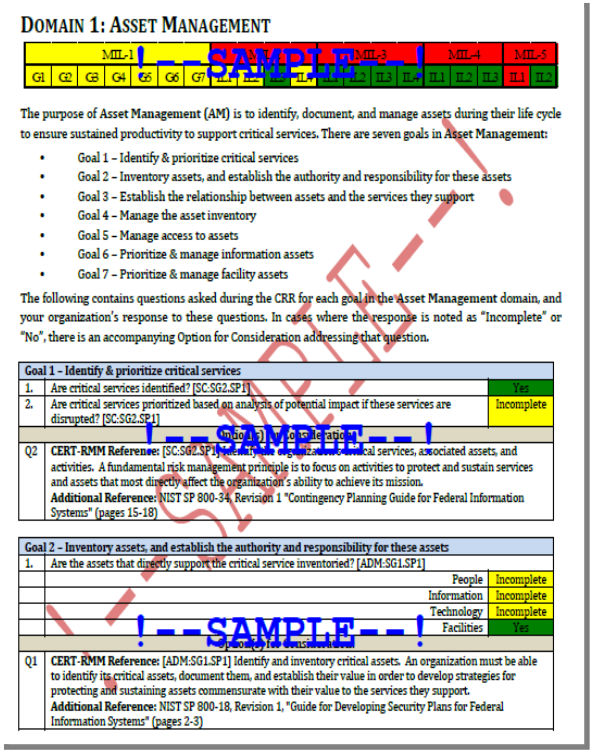
Each CRR report includes:



comparison data with other CRR participants
**facilitated only*

A summary "snapshot" graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses



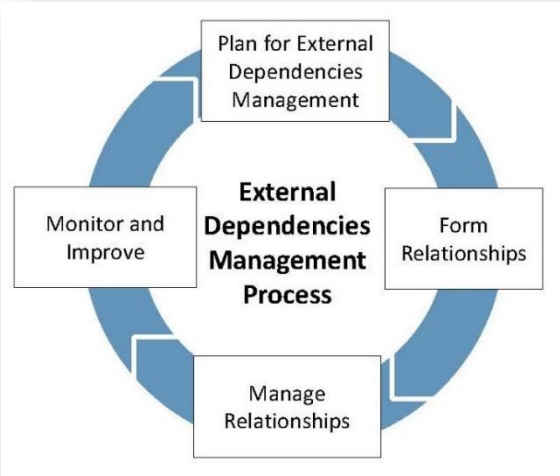
EXTERNAL DEPENDENCIES MANAGEMENT (EDM) ASSESSMENT

EDM Assessment Organization and Structure

- Structure and scoring very similar to DHS Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

Lifecycle

RF	**Relationship Formation** *The purpose of Relationship Formation is to assess whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
RMG	**Relationship Management and Governance** *The purpose of Relationship Management and Governance is to assess whether the acquirer manages ongoing relationships to maintain the resilience of the critical service, and mitigate dependency risk.*
SPS	**Service Protection and Sustainment** *The purpose of the Service Protection and Sustainment Domain is to assess whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.*



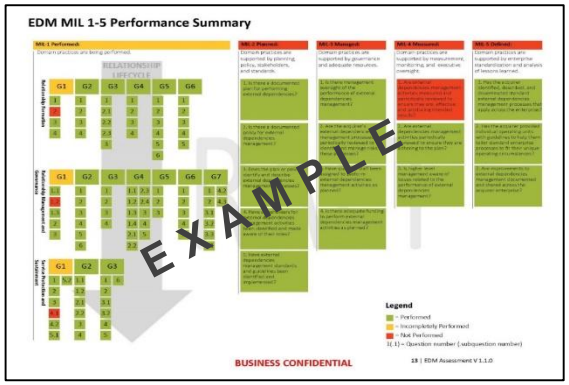
EDM process outlined in the External Dependencies Management Resource Guide

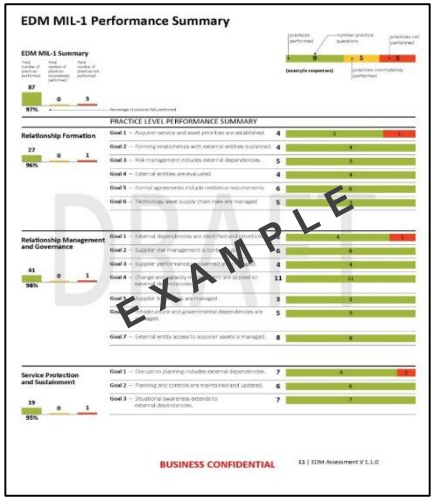
The EDM Assessment provides stakeholders with a more in-depth examination of risks associated with their third-party entities.

EDM Assessment Report

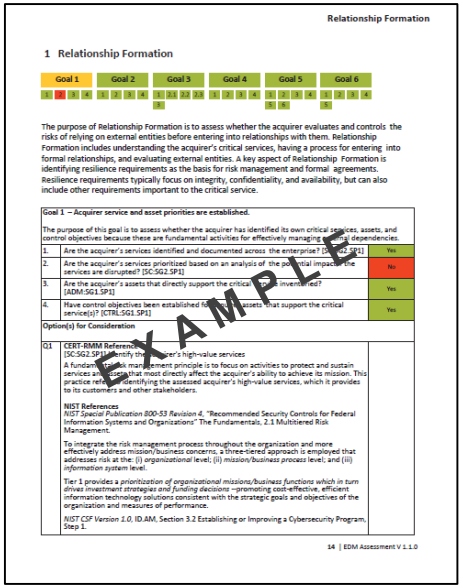
Each EDM report includes:

- Performance summary of existing capability managing external dependencies

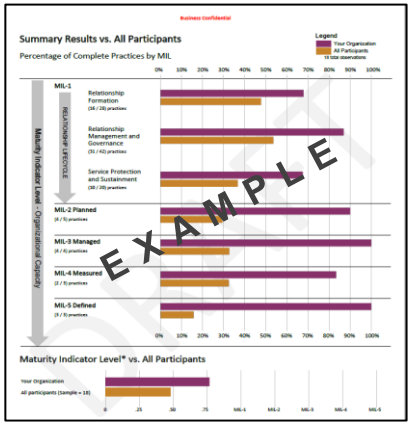




- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



- comparison data with other EDM participants



Homeland Security

CYBER INFRASTRUCTURE SURVEY (CIS)

CIS Dashboard

Scenario:
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

Threat-based PMI:
- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Cyber Security & Communications
Cyber IST Survey

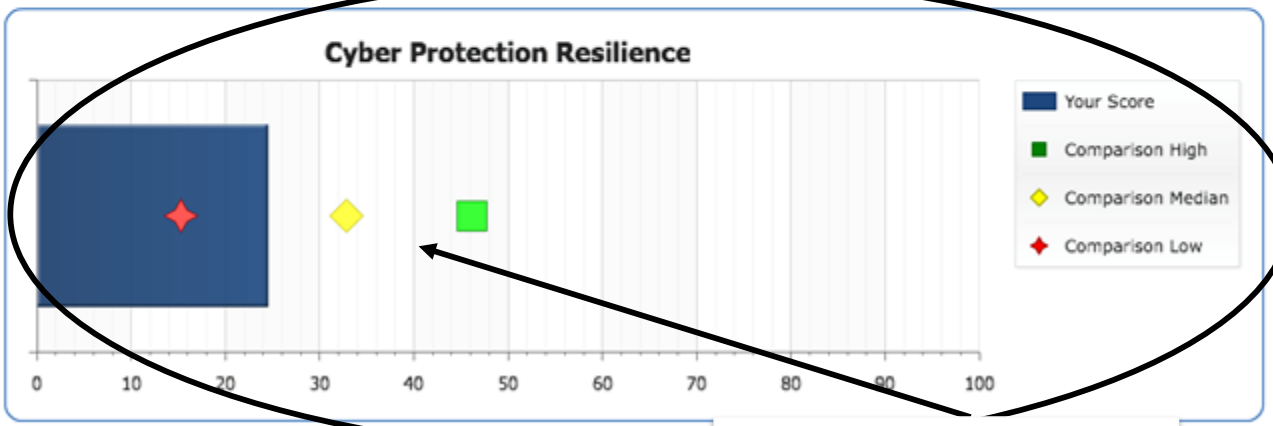
Home | Logout

Cyber IST Survey for

Threat Overlay: General Scenario: General

Cyber Protection Resilience Index
- Point Of Contact and Participants
- Critical Service Information
- **Cybersecurity Management**
- Cybersecurity Leadership
- Inventory
- System Architecture
- Security Architecture
- Change Management
- Lifecycle Tracking
- Accreditation and Assessment
- Cybersecurity Plan
- Cybersecurity Exercises
- External Information Sharing

Cyber Protection Resilience



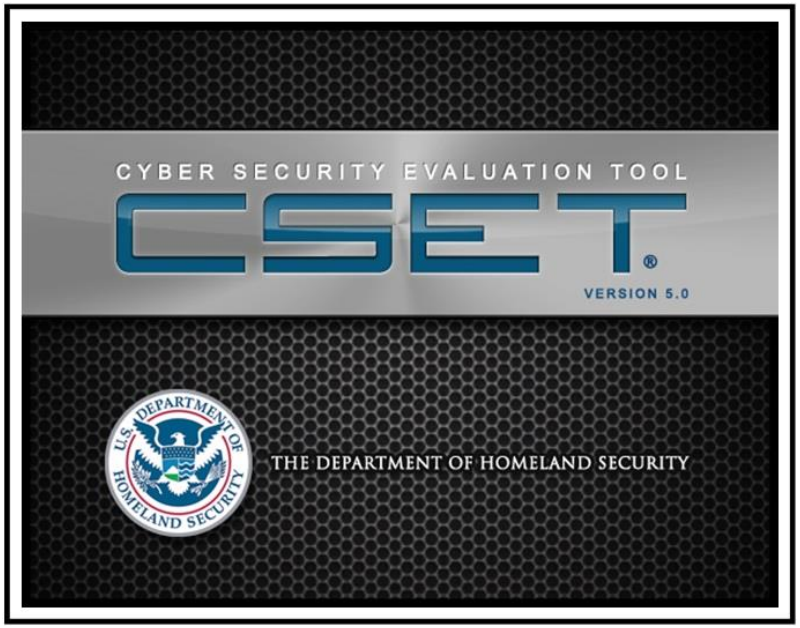
Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

Homeland Security

CYBER SECURITY EVALUATION TOOL (CSET)

Cyber Security Evaluation Tool (CSET ®)

- Stand-alone software application
- Self-assessment using recognized standards
- Tool for integrating cybersecurity into existing corporate risk management strategy



CSET Download:

http:/us-cert.gov/control_systems/csetdownload.html

PHISHING CAMPAIGN ASSESSMENT (PCA)

Phishing Campaign Assessment

Problem: Phishing is a common attack vector used to breach a stakeholder's operating environment and gain access to sensitive systems

Objectives:

- Increase cybersecurity awareness within stakeholder organizations
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation

Benefits:

- Receive actionable metrics
- Highlight need for improved security training

Phishing Campaign Assessment

Scope

- Phishing emails capture click-rate only, no payloads will be used
- Stakeholder provides a list of target users to receive custom crafted and approved phishing emails
  - Minimum 300, Maximum 7500
- 6-week engagement period

  Note: This is NOT a continuous assessment (there will be definitive start and end dates)
- Varying Levels of Complexity
  - Levels 1 - 6 (Easy to Difficult)
  - Complexity Level based on combination of indicator groups

Phishing Campaign Assessment

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@[PCA-testing-site].org> Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <fake link> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this programall we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114

Phishing Campaign Assessment

To: <Stakeholder List>

From: OBRM <OBRM@[PCA-testing-site].org>

Subject: Future Budget Plans

In the coming weeks, our state's leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

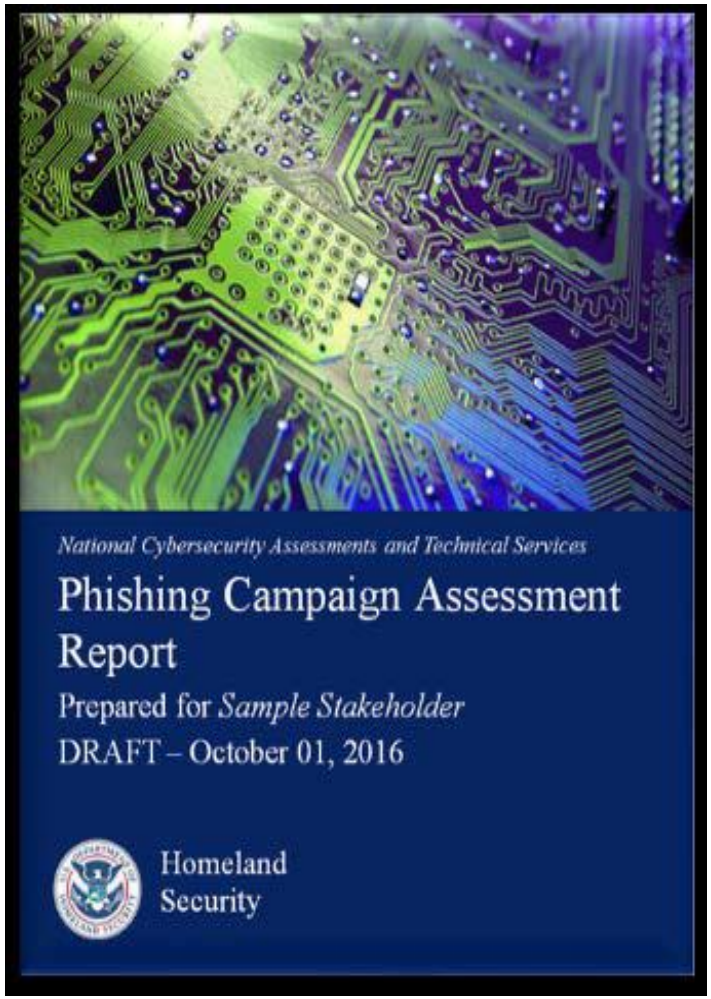
To learn more about the budget and how your program maybe affected, please visit <LINK>.

If you have any questions or concerns, we'd love to hear them. Please emails us here <embedded link>.

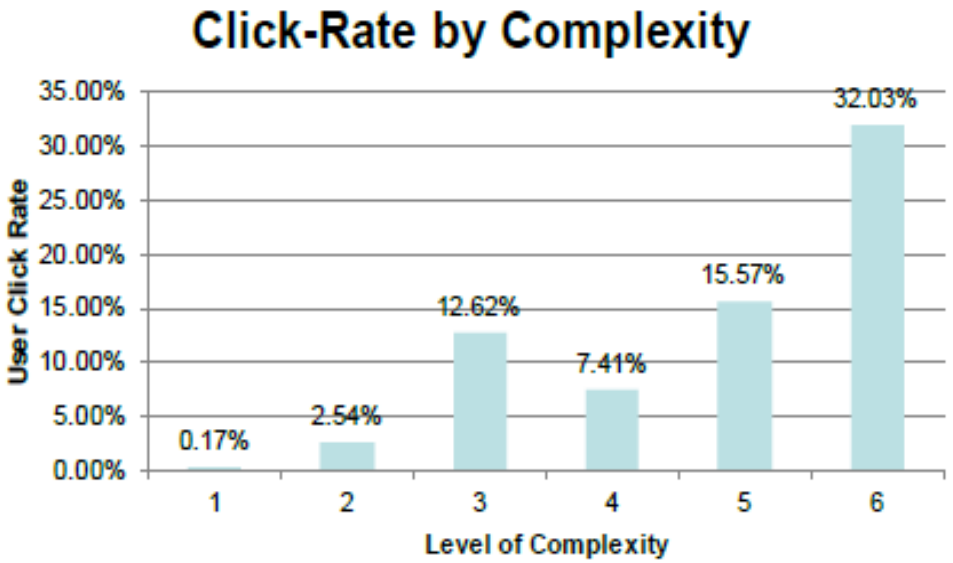
Office of Budget and Resource Management

Phishing Campaign Assessment

Sample Reports



Week	Campaign	Date Sent	Complexity Level	User Click Rate	# Emails Sent
1	Please Help!	3/18/16	1	0.17%	401
2	Reveal Your Past	3/31/16	2	2.54%	402
3	Password Expire Alert	4/6/16	3	12.62%	401
4	Severe Weather Checklist	4/15/16	4	7.41%	402
5	Federal Employee Survey	4/20/16	5	15.57%	401
6	Salary Guidelines	4/27/16	6	32.03%	402



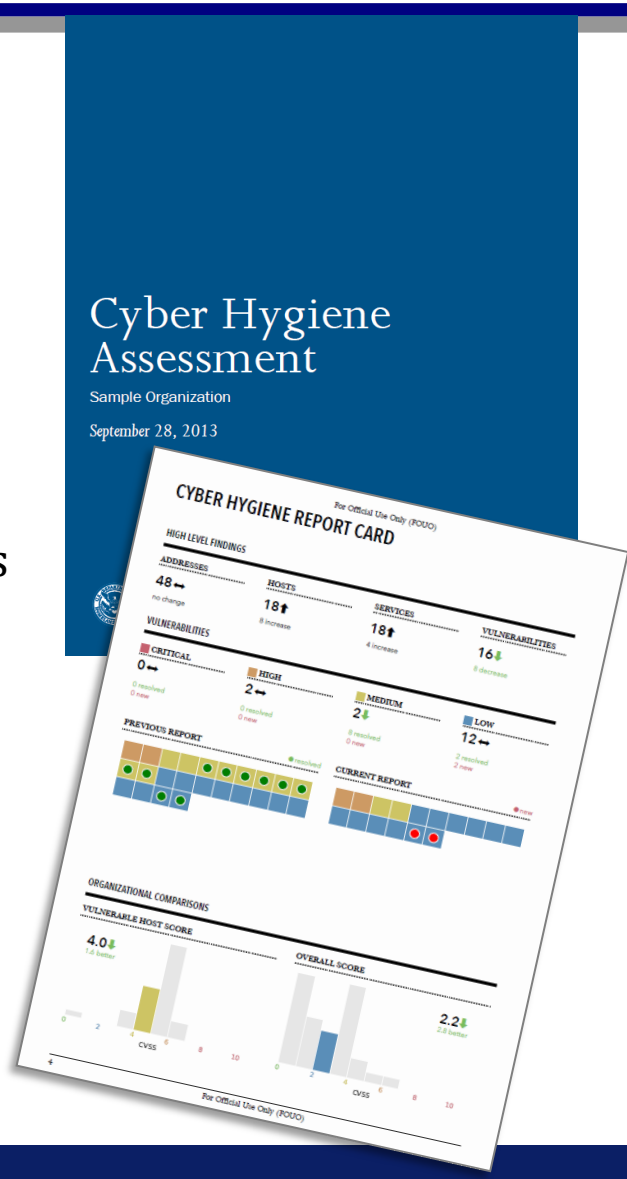
CYBER HYGIENE (CYHY)- VULNERABILITY SCANNING

CyHy - Vulnerability Scanning

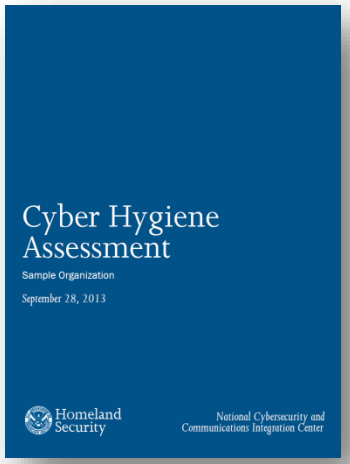
- Assess Internet accessible systems for known vulnerabilities and configuration errors.

- Work with organization to proactively mitigate threats and risks to systems. Activities include:
  - **Network Mapping**
    - Identify public IP address space
    - Identify hosts that are active on IP address space
    - Determine the O/S and Services running
    - Re-run scans to determine any changes
    - Graphically represent address space on a map

  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



CyHy - Vulnerability Scanning Sample Report Snapshots

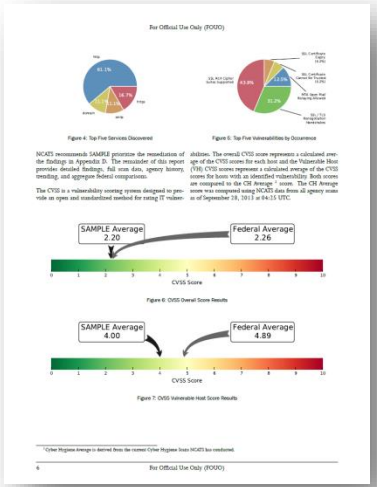

Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

National Cybersecurity and Communications Integration Center


For Official Use Only (FOUO)

SAMPLE Average 2.20

Federal Average 2.26

CVSS Score

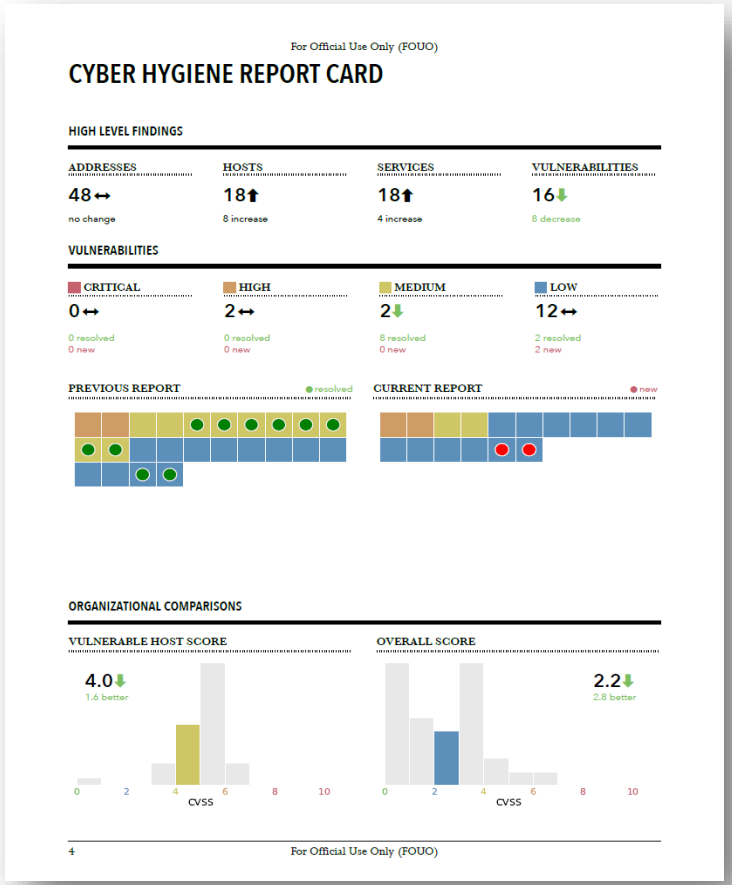
SAMPLE Average 4.00

Federal Average 4.89

CVSS Score

4

For Official Use Only (FOUO)


For Official Use Only (FOUO)

CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

ADDRESSES	HOSTS	SERVICES	VULNERABILITIES
48 ↔	18 ↑	18 ↑	16 ↓
no change	8 increase	4 increase	8 decrease

VULNERABILITIES

CRITICAL	HIGH	MEDIUM	LOW
0 ↔	2 ↔	2 ↓	12 ↔
0 resolved 0 new	0 resolved 0 new	8 resolved 0 new	2 resolved 2 new

PREVIOUS REPORT ● resolved

CURRENT REPORT ● new

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE

4.0 ↓

1.6 better

CVSS

OVERALL SCORE

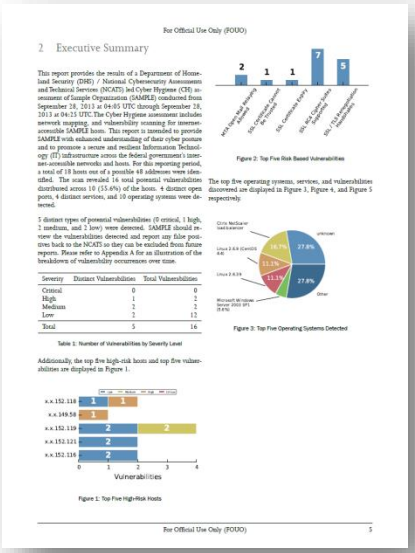
2.2 ↓

2.8 better

CVSS

4

For Official Use Only (FOUO)


For Official Use Only (FOUO)

2 Executive Summary

Figure 2: Top Five Risk Based Vulnerabilities

Figure 3: Top Five Operating Systems Detected

Table 1: Number of Vulnerabilities by Severity Level

Severity	Distinct Vulnerabilities	Total Vulnerabilities
Critical	0	0
High	1	2
Medium	2	2
Low	2	12
Total	5	16

Vulnerabilities

Figure 1: Top Five High-Risk Hosts

For Official Use Only (FOUO) 5

Homeland Security

VALIDATED ARCHITECTURE DESIGN REVIEW (VADR)

Validated Architecture Design Review

Purpose: Provides a sophisticated analysis of the asset owner's network architecture, system configurations, log file review, network traffic and data flows which can help to identify anomalous and communications

Deliverables: Six weeks after assessment completion, an in-depth report that includes an analysis of key discoveries and practical mitigations for enhancing the organization's cybersecurity posture. Report includes:

- Evaluation of network architecture
- Analysis of network traffic
- System log review and analysis
- Recommendations for improving an organization's operations

NETWORK RISK AND VULNERABILITY ASSESSMENTS (RVA)

[AKA, PEN TEST]

Homeland Security

Risk and Vulnerability Assessment (RVA)

- Conducts red-team assessments and provides remediation recommendations.
  - Identify risks, and provide risk mitigation and remediation strategies
  - Improves an agency's cybersecurity posture, limits exposure, reduces rates of exploitation, and increases the speed and effectiveness of future cyber attack responses.
- Services Include:

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of Operating System to do Compliance Checks

DHS CYBERSECURITY EVALUATIONS - SUMMARY - 1

Name	Cyber Resilience Review (CRR)	Cyber Infrastructure Survey (CIS)	External Dependency Management (EDM) Review	Onsite Cyber Security Evaluation Tool (CSET) Assessment
Purpose	Identify cyber security management capabilities and maturity	To calculate a comparative analysis and valuation of protective measures in-place	To assess the activities and practices utilized by an organization to manage risks arising from external dependencies.	Provides a detailed, effective, and repeatable methodology for assessing control systems security – while encompassing an organization's infrastructure, policies, and procedures.
Scope	Critical Service view	Critical Service view	Critical service view	Information Technology and Operational Technology systems
Time to Execute	8 Hours (1 business day)	2 ½ to 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours)/ N/A (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Capabilities and maturity indicators across third party relationship management lifecycle domains	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Short, 1-hour questionnaire plus planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager	IT / Security Manager with Continuity Planner and Contract Management	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts
Delivered By	CSAs cyberadvisor@hq.dhs.gov	CSAs cyberadvisor@hq.dhs.gov	CSAs cyberadvisor@hq.dhs.gov	Self-administered/ CSAs https://ics-cert.us-cert.gov/

DHS CYBERSECURITY EVALUATIONS – SUMMARY 2

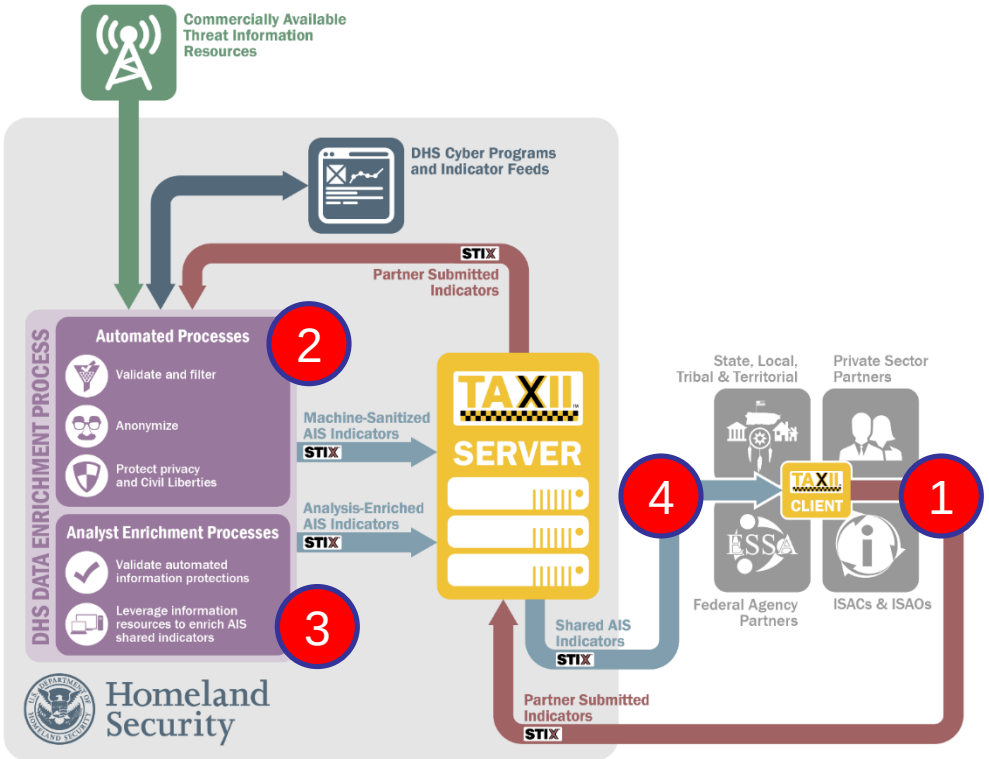
Name	Validated Architecture Design Review	Phishing Campaign Assessment (PCA)	Network Risk and Vulnerability Assessment (RVA)	Vulnerability Scanning
Purpose	Provides analysis and representation of asset owner's network traffic, data flows, and relationships between devices and identifies anomalous communications flows.	Measures the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems/ Network Architecture/ Network Traffic	Organization / Business Unit / Email Exchange Service	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, log files, data flows, interdependencies, and its applications	During the phishing assessment click rate metrics are gathered.	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Formal rules of engagement and pre-planning	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators, end users	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators
Delivered By	NCATS NCATS_INFO@hq.dhs.gov	NCATS NCATS_INFO@hq.dhs.gov	NCATs NCATS_INFO@hq.dhs.gov	NCATS NCATS_INFO@hq.dhs.gov

INFORMATION SHARING

Automated Indicator Sharing (AIS)

- The goal of AIS is to rapidly and widely share machine-readable cyber threat indicators and defensive measures at machine-speed for network defense purposes.

1. Entities format cyber threat indicators in STIX and submit via TAXII to DHS server.
2. Server code reviews submission to validate, anonymize (if requested), conduct automated privacy review and enrich.
3. Indicators requiring review go to DHS analysts.
4. Finally, indicators are published back out to everyone connected to the DHS server.



Additional Information Sharing Opportunities

- **Cyber Information Sharing and Collaboration Program (CISCP)**
  - Enhances cybersecurity collaboration between DHS and critical infrastructure owners and operators, and leverages government and industry subject matter expertise to collaboratively respond to cybersecurity incidents.
  - Supports data flow and analytical collaboration to support cyber threat information sharing across each of the 16 CI sectors.
  - Program provides participants with a range of timely and actionable products including threat/vulnerability indicators, early warnings and alerts focused on single threats/vulnerabilities expected to impact critical infrastructure, and recommended practices.
  - For more information about CISCP, please email ciscp_coordination@hq.dhs.gov.

- **DHS's Enhanced Cybersecurity Services (ECS) program**
  - Supports voluntary information sharing to assist and improve the protection of critical infrastructure systems from unauthorized access, exploitation, or data exfiltration. The program shares cyber threat information with qualified commercial service providers.
  - For more information about ECS, please visit the following url - http://www.dhs.gov/enhanced-cybersecurity-services, or email ECS_Program@HQ.DHS.gov.

Additional Information Sharing Opportunities:

- The Water ISAC is a non-profit water industry organization that delivers homeland security and preparedness information, including that regarding cybersecurity, to water and wastewater utilities and the government personnel who support them. Website: www.waterisac.org.

C³VP

- As part of Executive Order (EO) 13636, the Department of Homeland Security (DHS) developed the Critical Infrastructure Cyber Community Voluntary Program (C³VP).

- C3VP helps improve critical infrastructure cybersecurity and encourages organizations to adopt the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

us-cert.gov/ccubedvp

Contact Information

General Inquiries
cyberadvisor@hq.dhs.gov
C3VP:
us-cert.gov/ccubedvp

DHS Contact Information	
Tara Brewer	Tara.brewer@hq.dhs.gov Cell 202-875-3489

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications

Upcoming WaterISAC Events and Opportunities

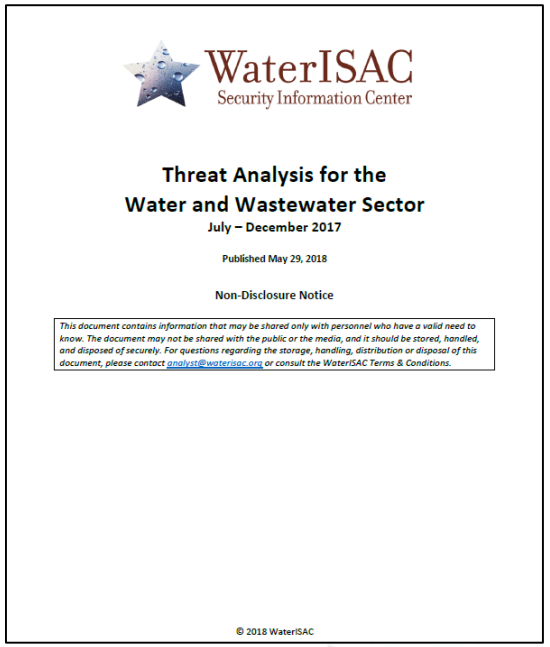
Monthly Cyber Threat Web Briefing

- Wednesday, July 25, 2018; 2:00 - 3:00 PM ET

Check the Events listing at WaterISAC and in the Pro Updates.

Semi-annual Water Sector Threat Analysis (January – June 2018)

- Survey will be active later today
- All survey respondents receive a copy


WaterISAC
Security Information Center

Threat Analysis for the Water and Wastewater Sector
July – December 2017

Published May 29, 2018

Non-Disclosure Notice

This document contains information that may be shared only with personnel who have a valid need to know. The document may not be shared with the public or the media, and it should be stored, handled, and disposed of securely. For questions regarding the storage, handling, distribution or disposal of this document, please contact analyst@watersac.org or consult the WaterISAC Terms & Conditions.

© 2018 WaterISAC

WaterISAC

Thank You

WaterISAC Contact Information:

1-866-H2O-ISAC

Michael Arceneaux
Managing Director
arceneaux@waterisac.org

Paul Laporte
Member Relations Manager
laporte@waterisac.org

Chuck Egli
Lead Analyst
egli@waterisac.org

Jennifer Walker
Cybersecurity Risk Analyst
walker@waterisac.org

WaterISAC