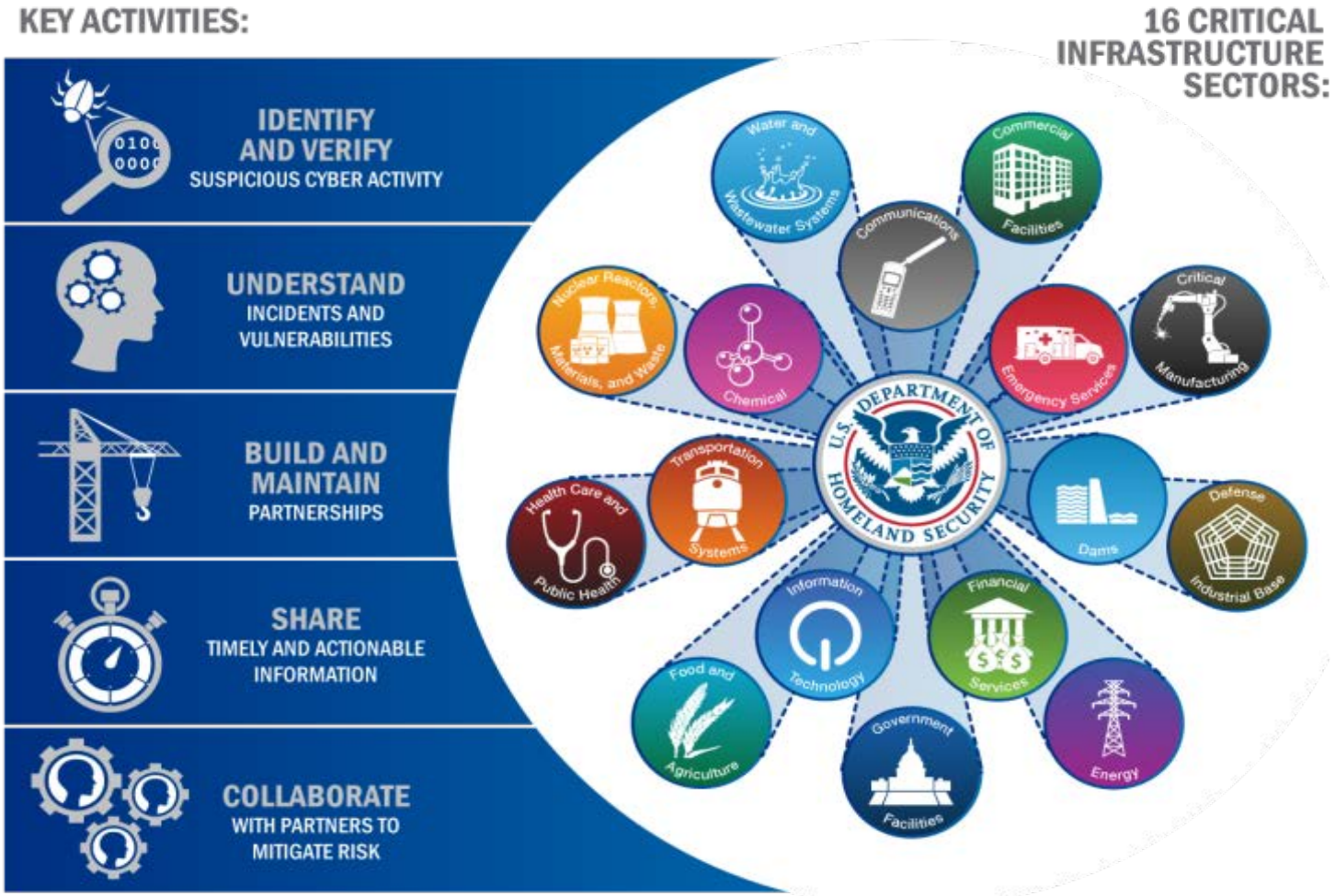
Homeland Security Perspectives:

Cyber Security Resources for Small and Medium-Sized Businesses

November 03, 2017

Ronald D. Watters Jr M.Ed GSLC
Cybersecurity Advisor Region X
Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR)
Cybersecurity and Communications (CS&C)

Critical Infrastructure (CI) Sectors

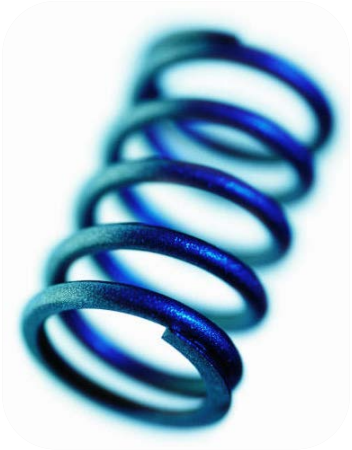


PLANNING FOR CYBER SECURITY IN A SMALL OR MEDIUM-SIZE BUSINESS

Homeland Security

What Is Cyber Resilience?

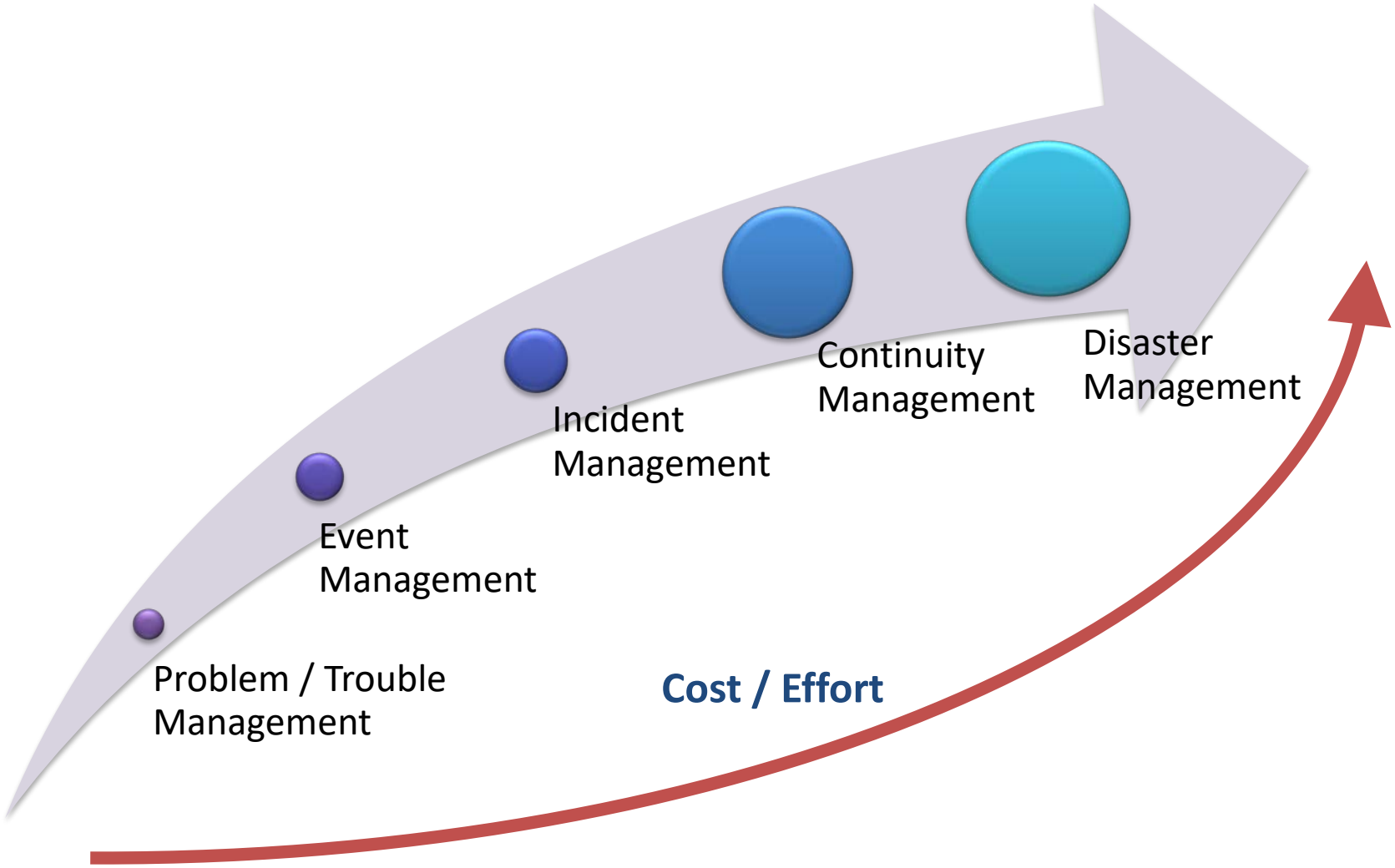
"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"



- Presidential Policy Directive – PPD 21
February 12, 2013

Protect (Security)	Sustain (Continuity)
Perform (Capability)	Repeat (Maturity)

Operational Planning for Cyber Security Events, Attacks, and Contingencies

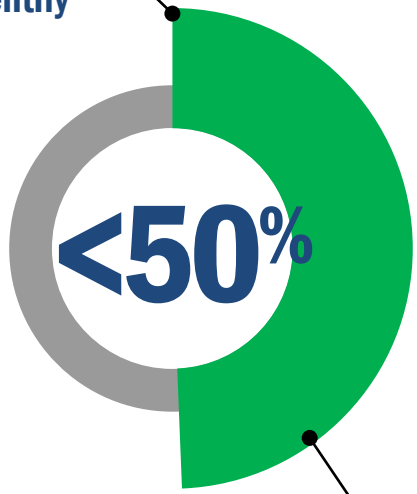


Take-Away #1

- Threat actors matter, in "Planning," so account for…
  - Method of attack can you detect, resist, and respond to…
  - How accurate you can determine how long they been "in" your systems and networks…
  - Their motivation: destruction, disruption, corruption, theft, etc…
- Be able to receive threat bulletins, advisories, and alerts from a "trusted" source… in addition to your own system and network monitoring
- Your technical and organizational response may only be sufficient depending on how well you know the technical perspective of the problem (i.e., attack and adversary)

DHS Cyber Resilience Review (CRR) Analytical Findings - 1

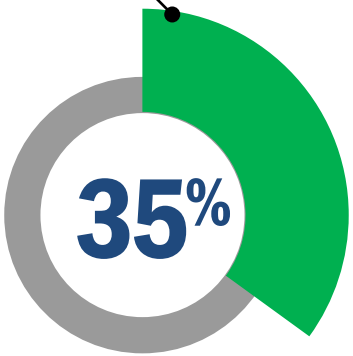
Less than half of organizations identify control objectives…

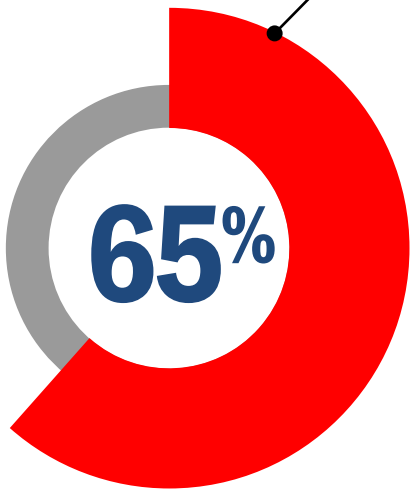


…and unfortunately less than half of those who identify control objectives, actually implement security controls to meet those objectives

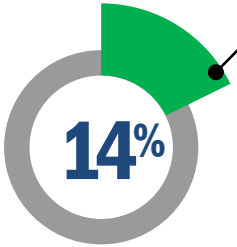
DHS CRR Analytical Findings - 2

Have a documented Vulnerability Management Plan





A majority (65%) of organizations lack a process to escalate and resolve incidents.



Have a documented Situational Awareness Plan

Take-Away #2

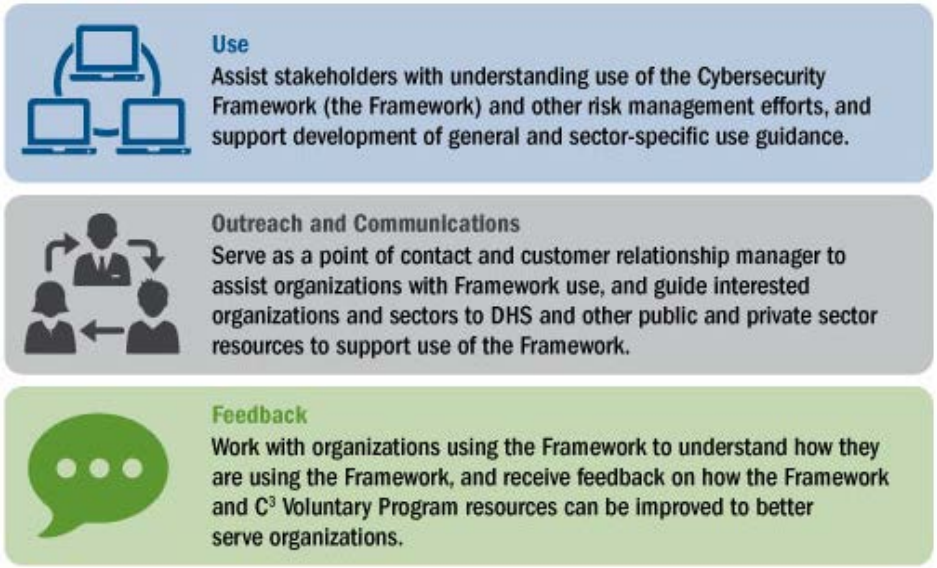
- Situational and operational awareness matter, in "Planning," so account for…
  - Method of attack can you detect, resist, and respond to…
  - How accurate you can determine how long they been "in" your systems and networks…
  - Their motivation: destruction, disruption, corruption, theft, etc…
- Understanding the "Gaps" in your system and network hardening, the status of security controls and vulnerabilities, and the configuration of your applications, operating systems, and security architecture may help you determine what happened (i.e., the likely attack path)
- An untested plan (incident, continuity, disaster, etc) is like having no plan…

RESOURCES FOR SMALL AND MEDIUM-SIZED BUSINESSES

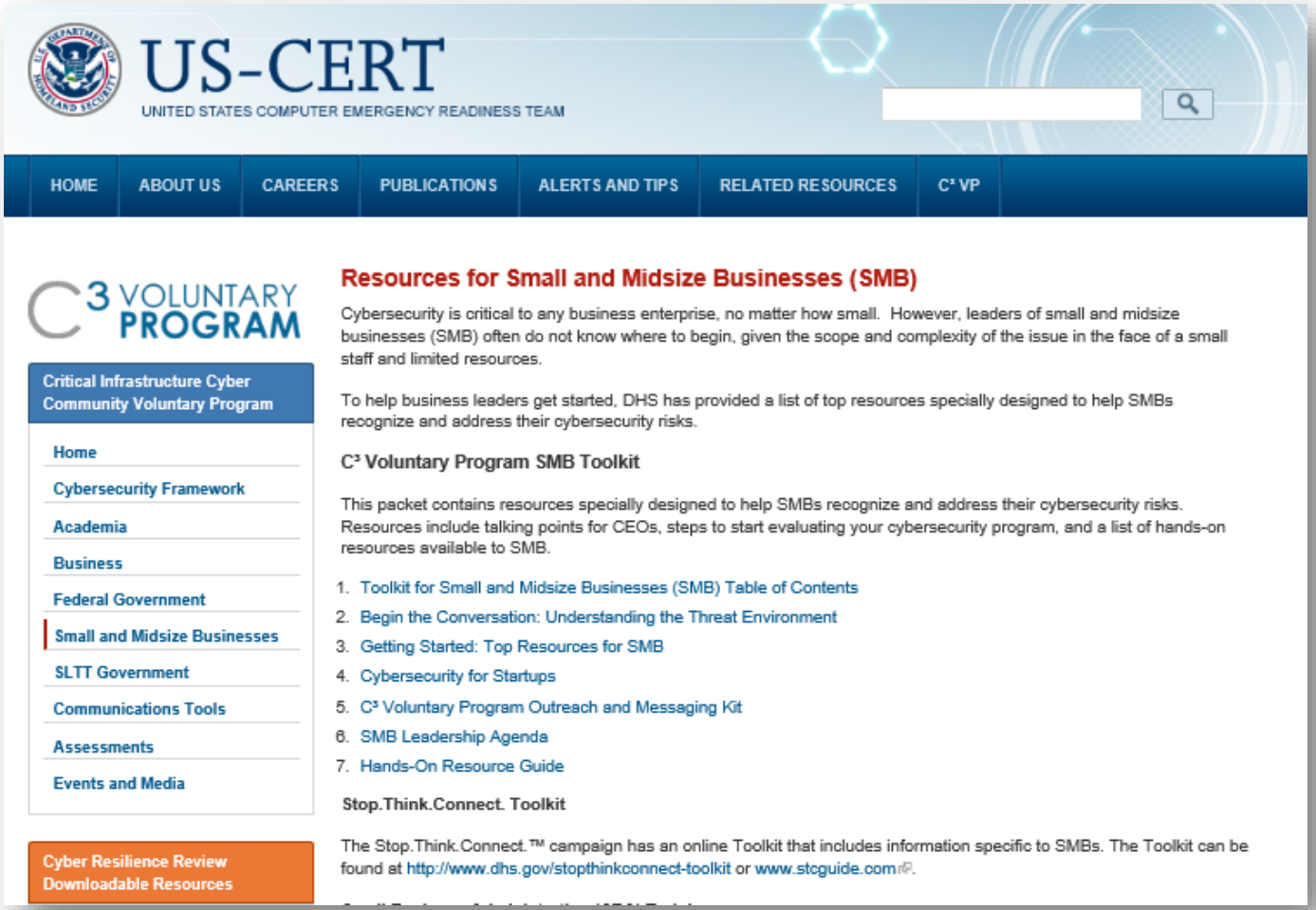
Implementation of the Cybersecurity Framework

Critical Infrastructure Cyber Community (C^3)

- In order to encourage use of the Framework, DHS has partnered with the critical infrastructure community to establish a voluntary program.
- The Critical Infrastructure Cyber Community (C^3) Voluntary Program is the coordination point within the Federal Government for critical infrastructure owners and operators interested in improving their cyber risk management processes. The C^3 Voluntary Program focuses on:

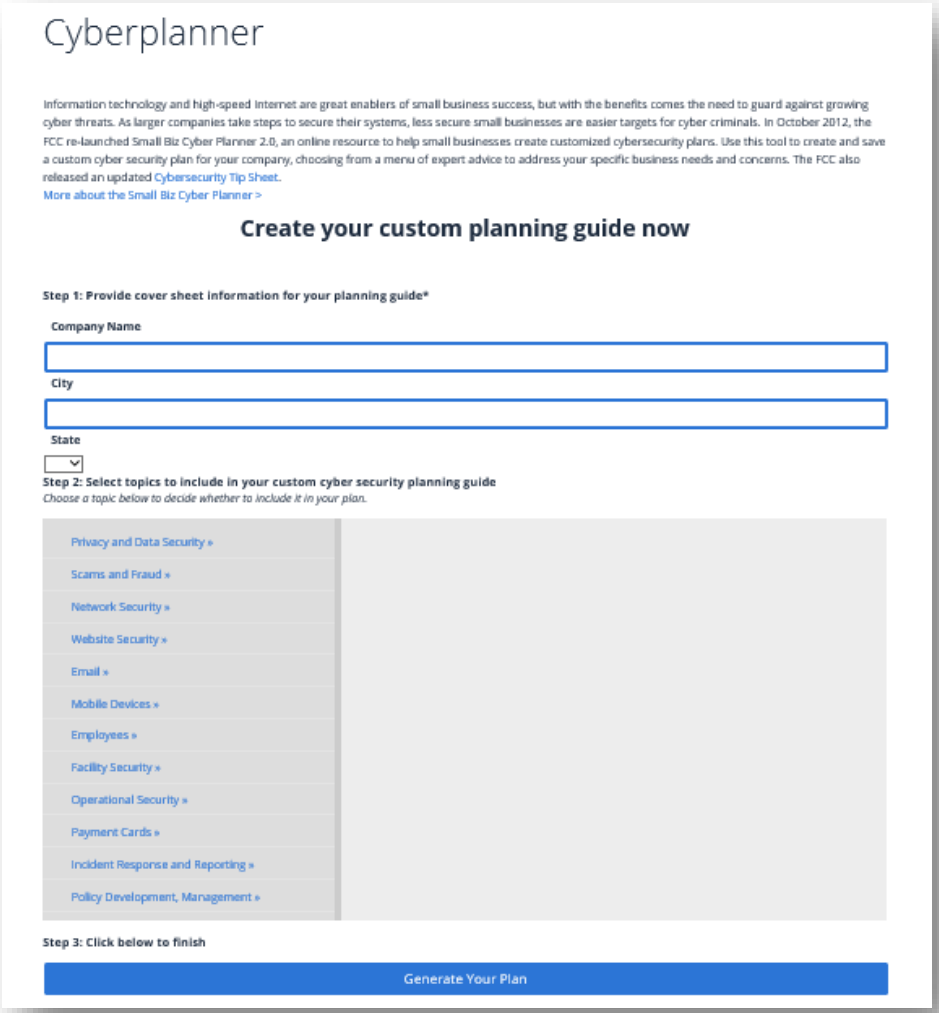


C³ Voluntary (Partner) Program Resources for Small and Medium-sized Businesses



https://www.us-cert.gov/ccubedvp/smb

FCC (Small Business-Oriented) *Cyberplanner*



"Click"-based cybersecurity planner, for:

- **Privacy and Data Security**
- **Scams and Fraud**
- **Network Security**
- **Website Security**
- **Email**
- **Mobile Devices**
- **Employees**
- **Facility Security**
- **Operational Security**
- **Payment Cards**
- **Incident Response and Reporting**
- **Policy Development, Management**

https://www.fcc.gov/cyberplanner

SBA Cybersecurity Resources

- Planning Guidance
- Training Resources
- Best Practices
- Tools and Self-Help Resources

https://www.sba.gov/managing-business/cybersecurity

SBA Top-10 Best Practices - 1

1. **Protect against viruses, spyware, and other malicious code**
   Make sure each of your business's computers are equipped with antivirus software and antispyware and update regularly.

2. **Secure your networks**
   Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden.

3. **Establish security practices and policies to protect sensitive information**
   Establish policies on how employees should handle and protect personally identifiable information and other sensitive data. Clearly outline the consequences of violating your business's cybersecurity policies.

4. **Educate employees about cyber threats and hold them accountable**
   Educate your employees about online threats and how to protect your business's data, including safe use of social networking sites. Depending on the nature of your business, employees might be introducing competitors to sensitive details about your firm's internal business.

5. **Require employees to use strong passwords and to change them often**
   Consider implementing multifactor authentication that requires additional information beyond a password to gain entry. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

https://www.sba.gov/managing-business/cybersecurity

SBA Top-10 Best Practices - 2

6. **Employ best practices on payment cards**
   Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor.

7. **Make backup copies of important business data and information**
   Regularly backup the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files.

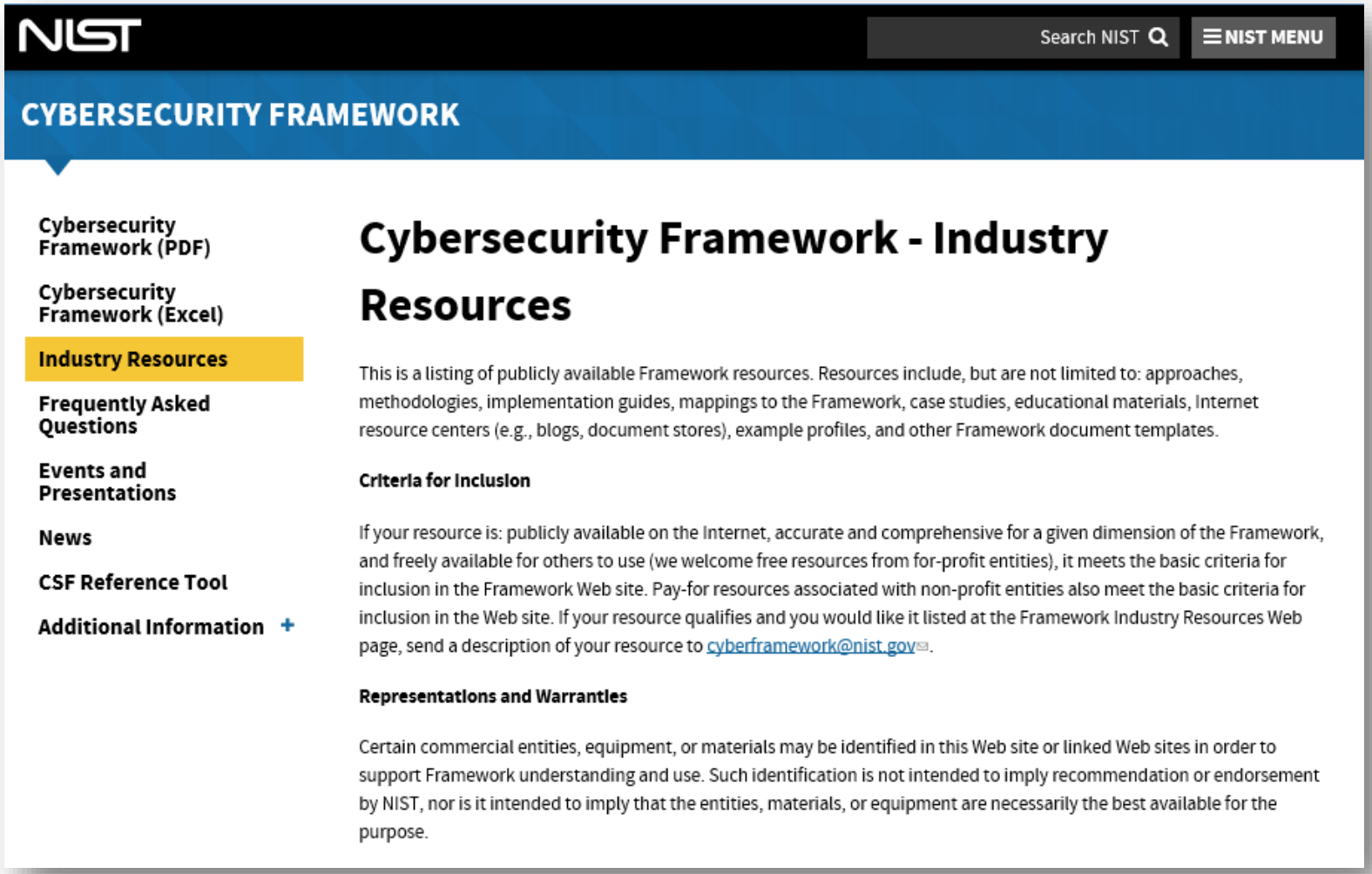
8. **Control physical access to computers and network components**
   Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended.

9. **Create a mobile device action plan**
   Mobile devices can create significant security and management challenges, especially if they hold confidential information or can access the corporate network.

10. **Protect all pages on your public-facing websites, not just the checkout and sign-up pages**

https://www.sba.gov/managing-business/cybersecurity

NIST Cybersecurity Framework (CSF) Resources



https://www.nist.gov/cyberframework/industry-resources

NIST list of Documents tha meet Controls Requirement

- **List of Compliance Docs for NIST 800-53 Ver. 4 Rev A**
  - Logical and Data Flow Diagrams
  - Copy of Current Authority to Operate (ATO) or Interim Authority to Operate (IATO)
  - Continuity of Operations Plan (COOP) or Contingency and Business Continuity Plan (CBCP) including identification of Mission Essential Elements
  - Evidence of having exercised the COOP
  - Disaster Recovery Plan (DRP)
  - Incident Response Plan (IRP)
  - Records of Incidents
  - Configuration Management (CM) Plan
  - Configuration Management Policy
  - Configuration Control Board (CCB) Charter
  - Service Level Agreements (SLAs)
  - Maintenance Contracts
  - Hardware Baseline Inventory
  - Software Baseline Inventory
  - Evidence of having undergone a Physical Penetration Test
  - Key Management Policy
  - Documented Open Storage Approval (where applicable)
  - IA Appointment Orders
  - Acceptable Use Policy (standard user) (AUP)
  - Acceptable Use Policy (Privileged User) (AUP/PUP)
  - IA Vulnerability Management (IAVM) Process/Procedures
  - Device Configuration files
  - Data at Rest (DAR) policy
  - Media Protection and Sanitization Policy
  - System Interface agreements (e.g. MOUs/MOAs) with other enclaves outside the accreditation boundary (including any tenants with their own ATO)
  - Role Based Access List (RBAC)
  - Access Control Policy/Account Creation Policy
  - Site Security Plan (SSP)
  - Audit and Accountability Policy
  - Vulnerability Scan / SOP
  - Maintenance Policy

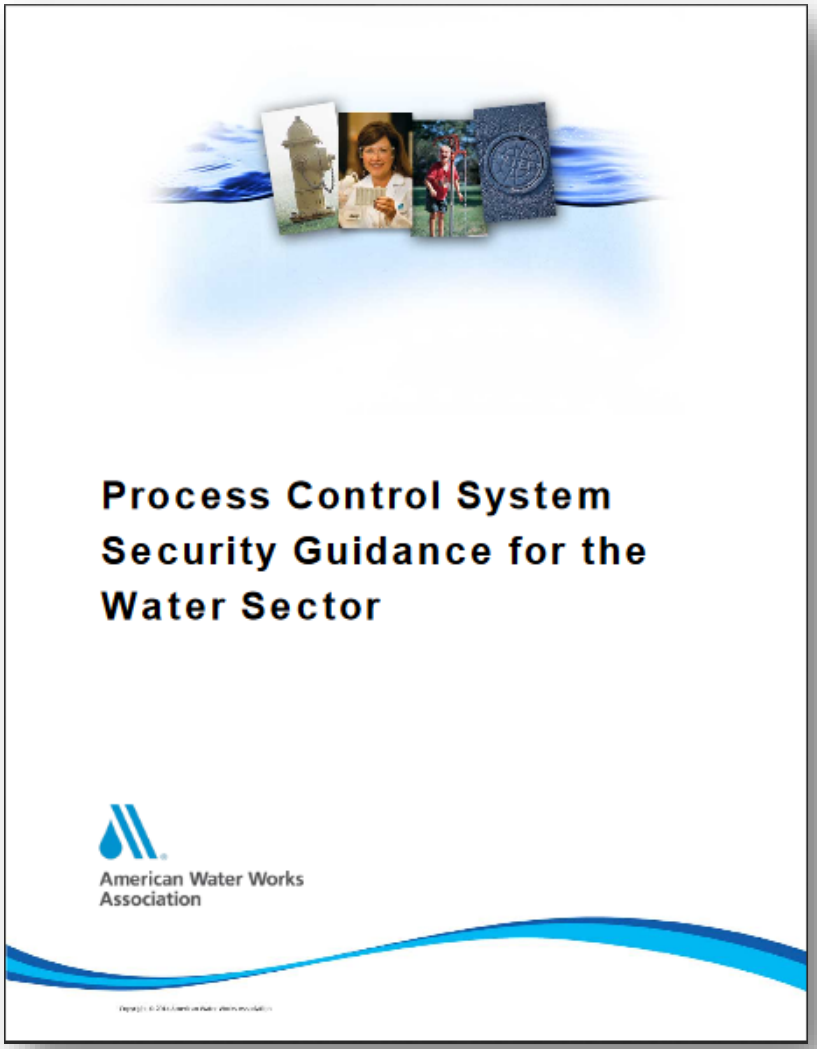
Analysis Paralysis

- PSUEDO Medical term for “Brain Freeze” when faced with multiple critical projects or objectives leading to failure to complete any.
  - Take one item at a time and complete it, chip away at the problem one step at a time.
    - Advantage is that you can show progress completing tasks
    - Disadvantage is that it takes more planning and time.
  - Plan and Budget for ongoing projects
    - You are not going to be able to complete major infrastructure projects quickly, so plan and prepare.
    - Convene a Configuration Change Management meeting to discuss and have plan approved far in advance of actual commencement of work.
    - Move expensive portions to the next Fiscal year and budget for them.

Analysis Paralysis

- Develop Partnerships
  - There is a wealth of resources available to assist with your plans, you just need to find them.
  - Build a relationship with your CSA (ME)
  - Contact your Fusion Center
  - Become involved with INFRAGARD
  - Become involved with you local Cyber Groups
  - Partner with business in your area

American Water Works Association – [Cybersecurity] Process Control System Guidance



1. Governance and Risk Management
2. Business Continuity and Disaster Recovery
3. Server and Workstation Hardening
4. Access Control
5. Application Security
6. Encryption
7. Telecommunications, Network Security, and Architecture
8. Physical Security of PCS Equipment
9. Service Level Agreements (SLA)
10. Operations Security (OPSEC)
11. Education
12. Personnel Security

http://www.awwa.org/

AWWA Cybersecurity Tool

- Provides an online and ready-resource for cybersecurity planning
  - Uses Use-Case scenarios
  - A literal “Choose-Your-Own-Adventure” in cybersecurity
  - Aligns to NIST SP800-82 and other recognized standards

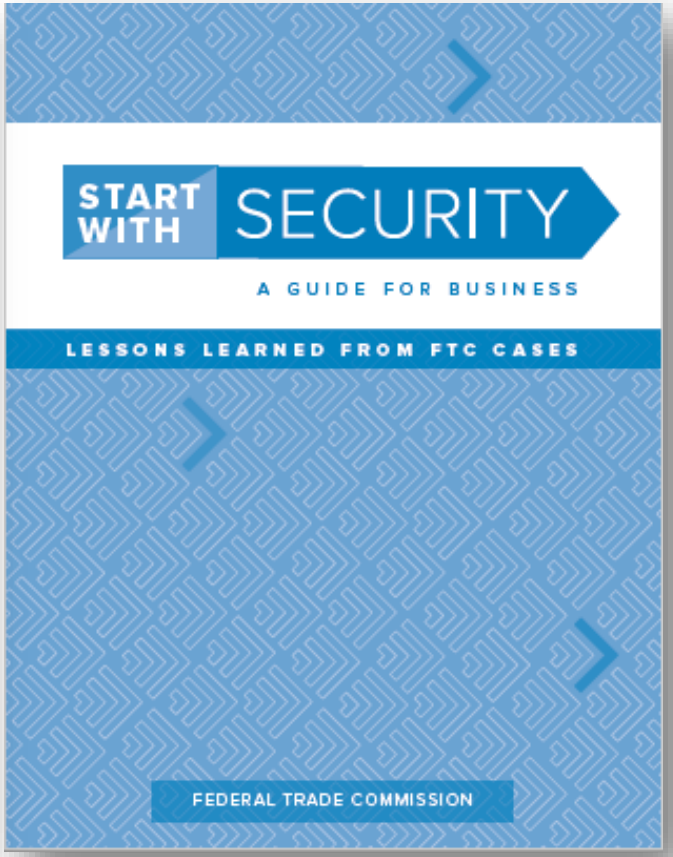
- Provides a dynamic and interactive reporting tool, with information reported on both must-have and nice-to-have controls (i.e., priority 1 – basic due diligence to priority 4 – compensating)

- Does not assess what is in place – you need to “red-line” those practices already implemented

http://www.awwa.org/resources-tools/water-and-wastewater-utility-management/cybersecurity-guidance.aspx

FTC – Guidance and Resources

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security



https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf

DHS (FREE) CYBER SECURITY EVALUATIONS: OVERVIEWS

- CYBER RESILIENCE REVIEW (CRR)
- CYBER INFRASTRUCTURE SURVEY TOOL (C-IST)
- CYBER HYGIENE

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - **Remote / On-Site Assistance**
    - **Malware Analysis**
    - **Incident Response Teams**
  - ICS-CERT Operations Center
    - **ICS-CERT Malware Lab**
    - **Incident Response Teams**
  - Cyber Exercise Program
- Cyber Security Advisors
- Protective Security Advisors

- Preparedness Activities
  - **National Cyber Awareness System**
  - **Vulnerability Notes Database**
  - **Security Publications**
  - **Technical Threat Indicators**
  - **Cybersecurity Training**
  - **Information Products and Recommended Practices**
- Control Systems Evaluations
  - **Cyber Security Evaluation Tool**
  - **ICS Design Architecture Reviews / Network Architecture Analysis**
- Other Cyber Security Evaluations
  - **Cyber Resilience Review**
  - **Cyber Infrastructure Survey Tool**
  - **Cyber Hygiene service**
  - **Risk and Vulnerability Assessment (aka "Pen" Test)**
  - **Phising Vulnerability Assessment**

CYBER RESILIENCE REVIEW (CRR)

Cyber Resilience Review (CRR) - 1

Helps CIKR (Critical Infrastructure and Key Resources) and SLTT (State, Local, Tribal and Territorial) partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk during:

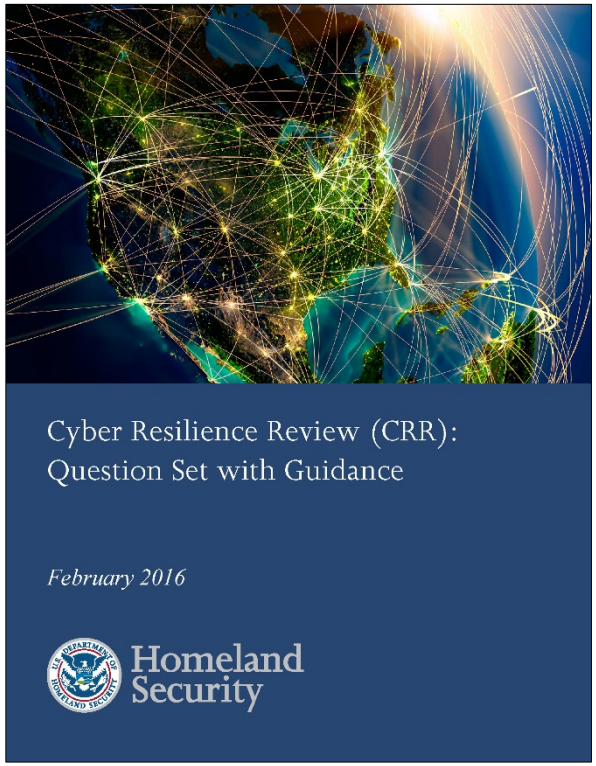
- normal operations (i.e., protection & sustainment)
- times of operational stress and crisis (i.e., survivability & resilience)

Based on the CERT ® Resilience Management Model (CERT® RMM), a process improvement model for managing operational resilience

- Cross-referenced and compatible with the NIST Security Management Framework (i.e., EO 13636)

Cyber Resilience Review (CRR) - 2

- **Purpose:** The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices across **ten foundational** cybersecurity domains.
- **Delivery:** The CRR can be **facilitated** by a DHS cybersecurity professional (e.g., Cyber Security Advisor) or **self-administered** by organizations utilizing the CRR Self-Assessment Package.
- **Output:** The CRR provides organizations with a report detailing its capability and maturity in security management, and gaps against **NIST Cyber Security Framework**.
- **Scope:** The CRR is a voluntary assessment that is available at **no cost** to requesting organizations.



CRR Question Set & Guidance

The CRR provides organizations with a no-cost method to assess their cybersecurity postures

CRR 10 Domains

- ASSET MANAGEMENT
- CONTROLS MANAGEMENT
- CONFIGURATION AND CHANGE MANAGEMENT
- VULNERABILITY MANAGEMENT
- INCIDENT MANAGEMENT
- SERVICE CONTINUITY MANAGEMENT
- RISK MANAGEMENT
- EXTERNAL DEPENDENCY MANAGEMENT
- TRAINING AND AWARENESS
- SITUATIONAL AWARENESS

Recent Developments: Self-Assessment Package

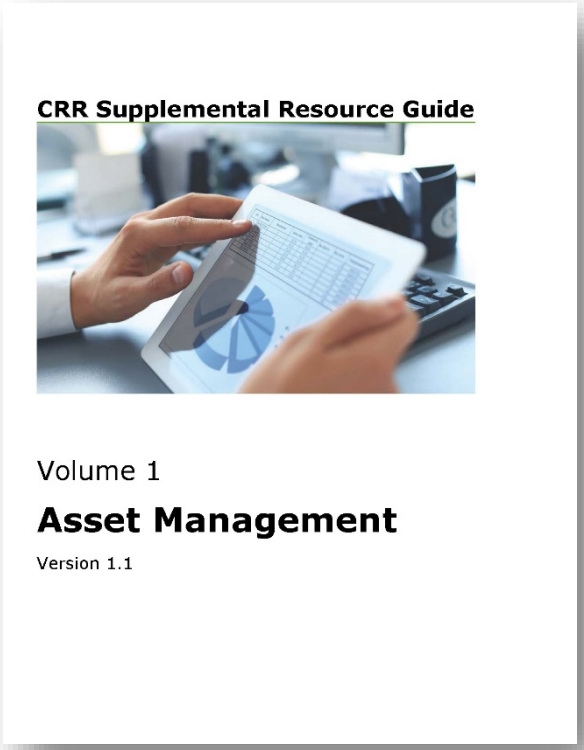
- **Overview:** The CRR Self-Assessment provides a means through which organizations can conduct a CRR without the particip facilitators.
- **Recent Updates**: In February 2016, DHS released V Self-Assessment Package. Key updates included:
  - New and modified questions, incorporating practices “snapshot” graphic, related to the **NIST Cyber Secu**
  - Available as a complete self-administered package Voluntary Program website at: https://www.us-cert.gov/ccubedvp/assessments/.
  - Participant ability to add comparison data to self-ass when organizations share self-administered results purpose.

Example scoring overview from a CRR Self-Assessment

Version 2.0 of the CRR Self-Assessment offers an updated question set and enhanced linkage with the NIST Cyber Security Framework.

Recent Developments: Resource Guides

- **CRR Domains**: The CRR methodology is based on 10 “domains,” each representing a capability area foundational to an organization’s cyber resilience.
- **Resource Guides**: In 2016, DHS released a set of CRR Resource Guides to assist organizations in enhancing their resilience in specific CRR domains.
- **Scope of Content**: While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use**: Moreover, the guides can be utilized as a full set or as individual



CRR Resource Guide – Asset Management

CRR Resource Guides provide organizations with a tool to develop their capabilities in security management areas – moving organizations from initial to well-defined capability.

CYBER INFRASTRUCTURE SURVEY TOOL (C-IST)

Cyber IST Highlights

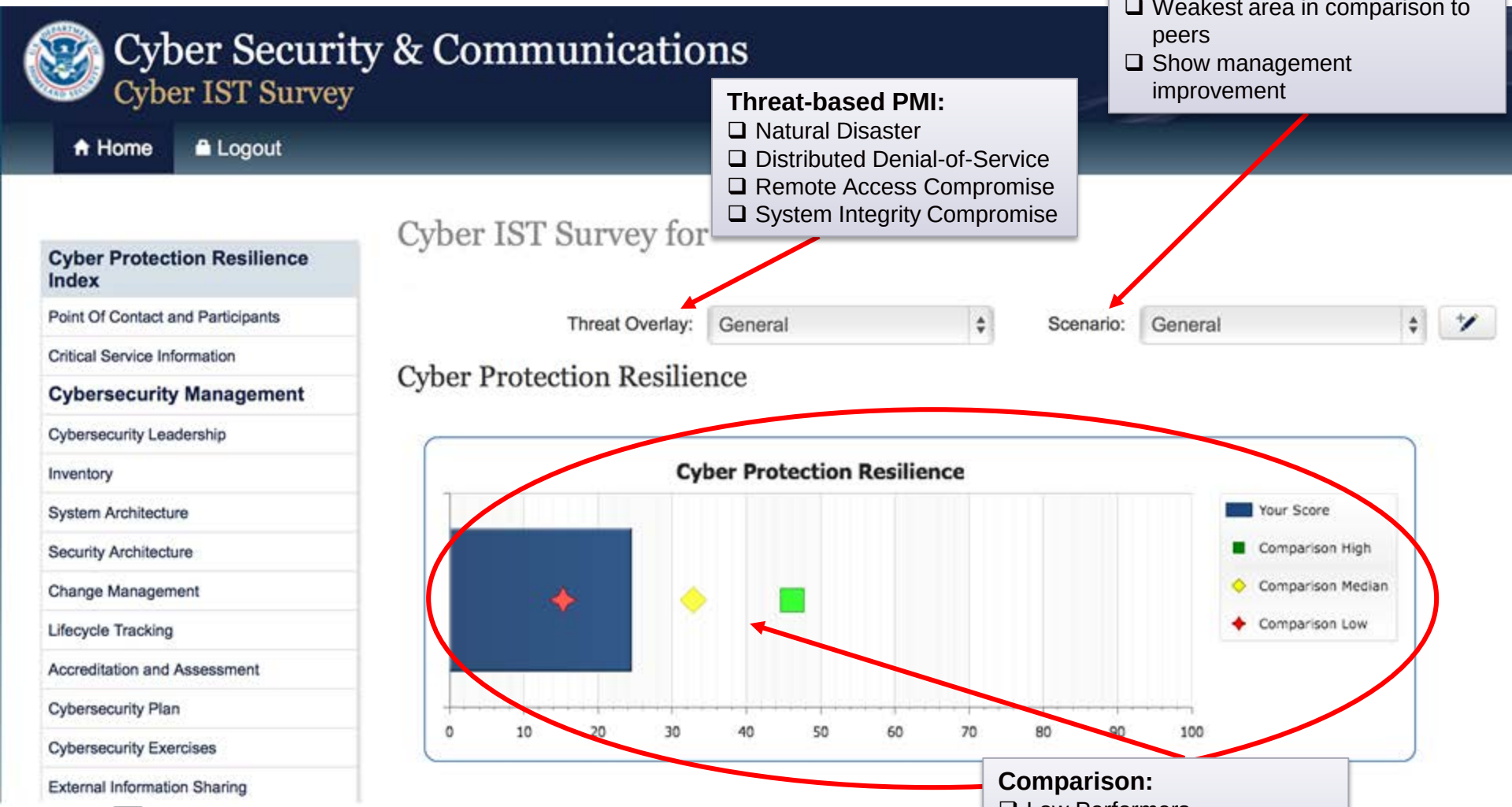
	Facts and Talking Points	Notes / Examples
Purpose	To calculate a comparative analysis and valuation of protective cyber security measures in-place	The Cyber IST is a survey instrument -- useful in limited situations, such as: • With new and potential partner organizations, as a relationship starter (i.e., introduction to DHS critical cyber infrastructure protection) • With existing partners, as a light-weight evaluation activity (i.e., produces no formal report and no formal recommendations)
Scope	Critical service view	• Electronic Medical Records System • Water Filtration Control Network and SCADA System
Time to Execute	2 ½ to 4 Hours	Pilot experience demonstrated 2 ½ hours is minimum requirement; however, at 2 ½ hours the evaluation neither is "rushed" nor allows for extended discussions
Information Sought	Protective measures in-place	Five core areas are measures: • Cyber Security Management • Cyber Security Forces (aka Personnel) • Cyber Security Controls • Incident Response and Continuity • Cyber Dependencies
Preparation	Planning call or discussion	Extensive planning is unnecessary, but a pre-conversation can be useful to: • Gauge and confirm interest • Select a critical service • Gather demographic information
Participants	IT/Security Manager	• The survey nature of the assessment lends itself best to a limited number of participants (i.e., 1-2 interviewees) • If additional information is needed, the protocol should be to allow for the primary POC to collect the missing information

Homeland Security

Example of C-IST 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

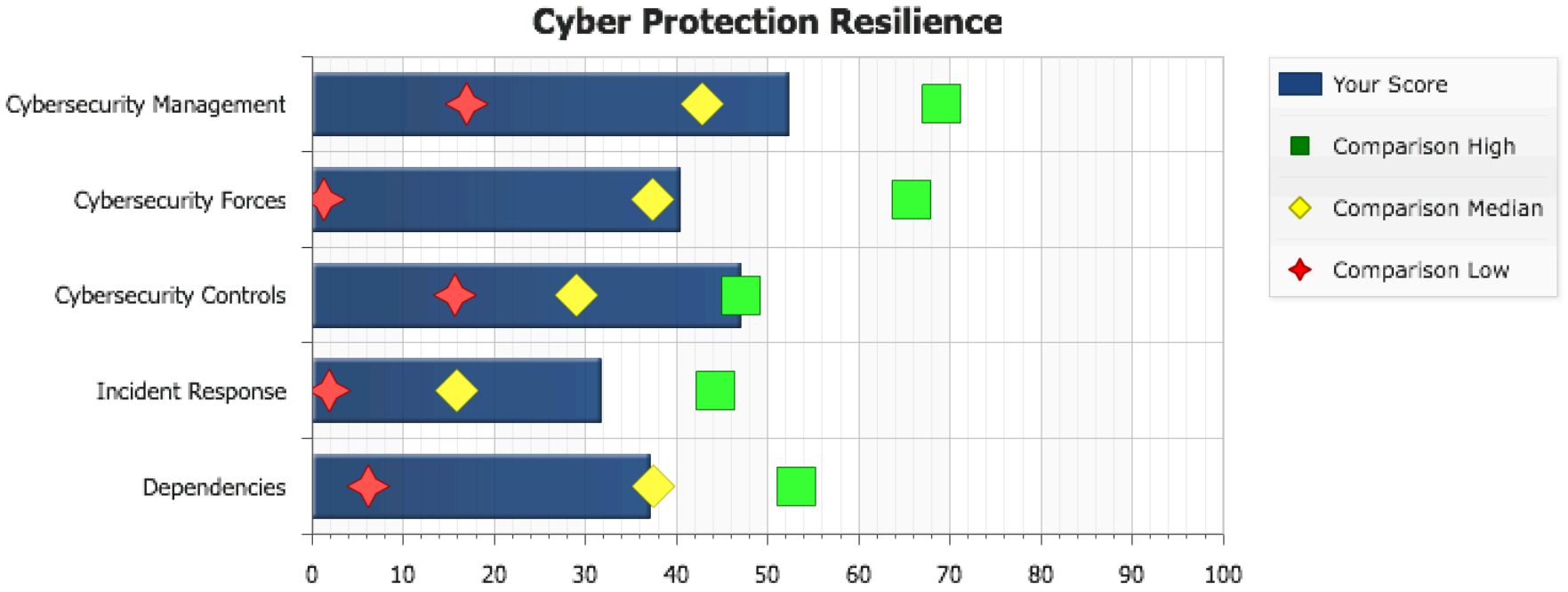


Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

Homeland Security

C-IST Dashboard - Comparison

- Shows the low, median, and high performers



Homeland Security

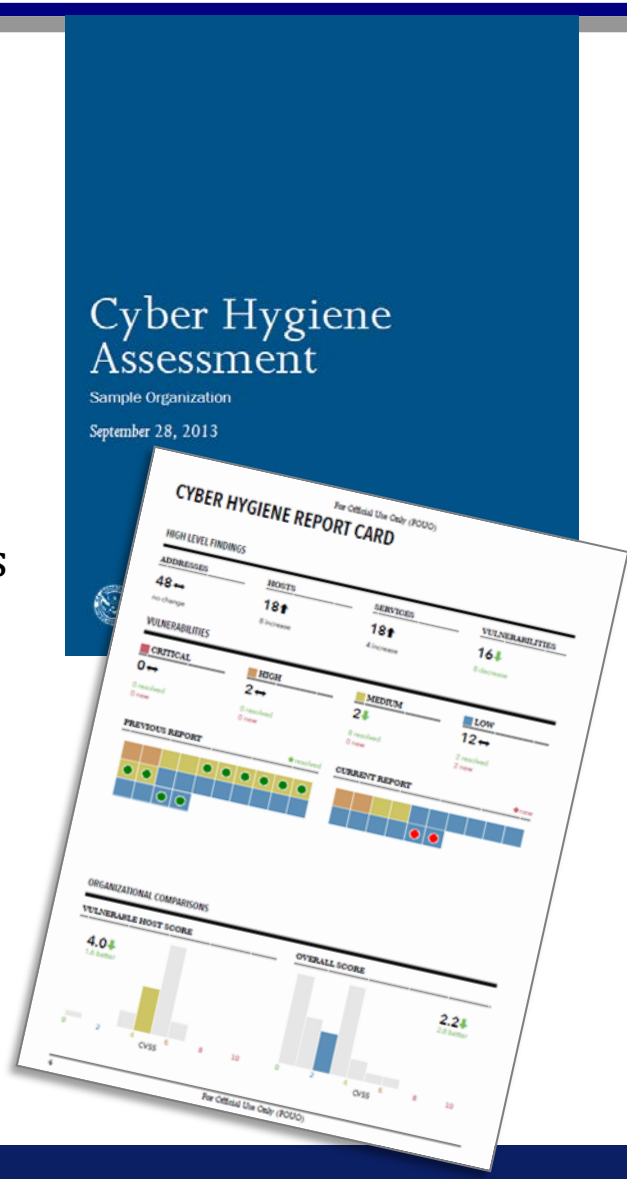
CYBER HYGIENE (CYHY)

Cyber Hygiene

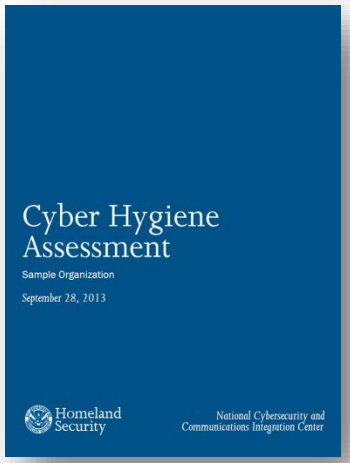
- Assess Internet accessible systems for known vulnerabilities and configuration errors.

- 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™ Sample Report Snapshots


Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

National Cybersecurity and Communications Integration Center

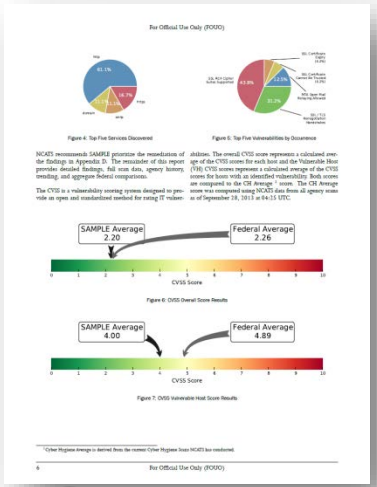

For Official Use Only (FOUO)

Figure 4: Top Five Services Discovered

Figure 5: Top Five Vulnerabilities by Occurrence

NCATS recommends SAMPLE prioritize the remediation of the findings in Appendix D. The remainder of this report provides detailed findings, full scan data, agency history, trending, and aggregate federal comparisons.

The CVSS is a vulnerability scoring system designed to provide an open and standardized method for rating IT vulnerabilities. The overall CVSS score represents a calculated average of the CVSS scores for each host and the Vulnerable Host (VH) CVSS scores represents a calculated average of the CVSS scores for hosts with an identified vulnerability. Both scores are compared to the CH Average [1] score. The CH Average score was computed using NCATS data from all agency scans as of September 28, 2013 at 04:15 UTC.

SAMPLE Average 2.20

Federal Average 2.26

CVSS Score

Figure 6: CVSS Overall Score Results

SAMPLE Average 4.00

Federal Average 4.89

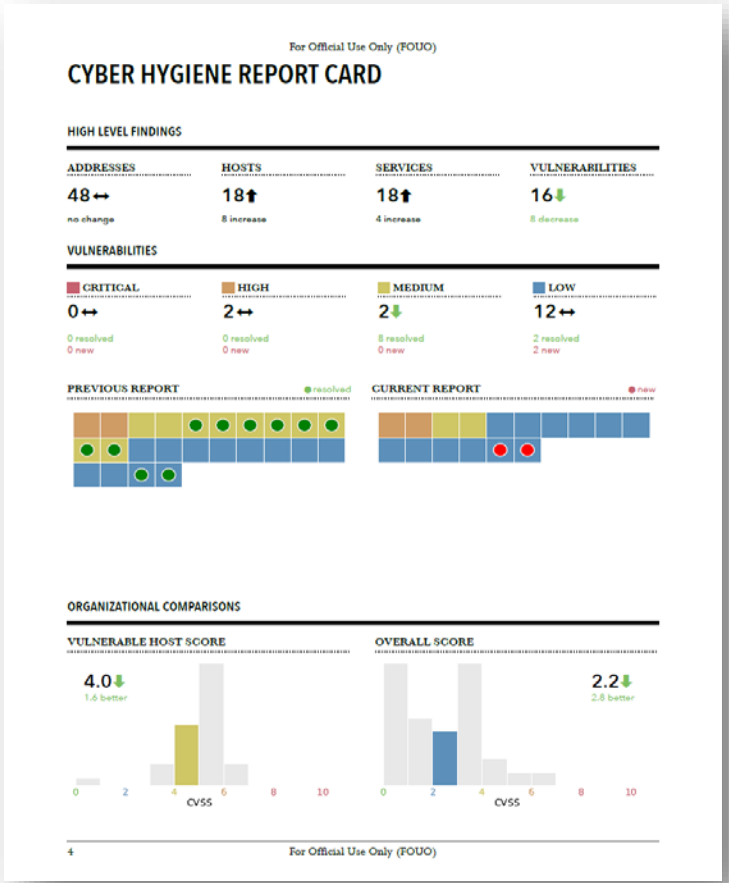
CVSS Score

Figure 7: CVSS Vulnerable Host Score Results

[1] Cyber Hygiene Average is derived from the current Cyber Hygiene Scans NCATS has conducted.

6

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

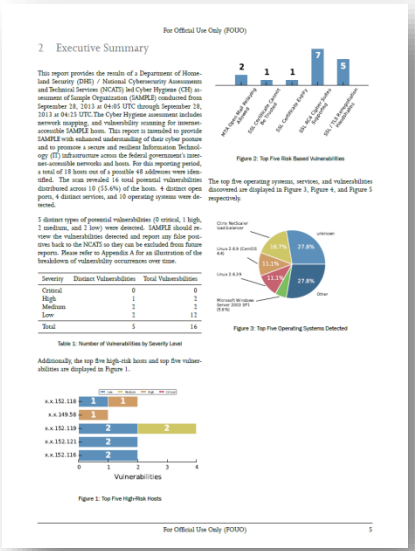
2.2 ↓

2.8 better

CVSS

4

For Official Use Only (FOUO)


For Official Use Only (FOUO)

2 Executive Summary

This report provides the results of a Department of Homeland Security (DHS) / National Cybersecurity Assessment and Technical Services (NCATS) led Cyber Hygiene (CH) assessment of Sample Organization (SAMPLE) conducted from September 28, 2013 at 04:05 UTC through September 28, 2013 at 04:25 UTC. The Cyber Hygiene assessment includes network mapping, and vulnerability scanning for internet-accessible SAMPLE hosts. This report is intended to provide SAMPLE with enhanced understanding of their cyber posture and to promote a secure and resilient Information Technology (IT) infrastructure across the federal government's internet-accessible networks and hosts. For this reporting period, a total of 18 hosts out of a possible 48 addresses were identified. The scan revealed 16 total potential vulnerabilities distributed across 10 (55.6%) of the hosts. 4 distinct open ports, 4 distinct services, and 10 operating systems were detected.

5 distinct types of potential vulnerabilities (0 critical, 1 high, 2 medium, and 2 low) were detected. SAMPLE should review the vulnerabilities detected and report any false positives back to the NCATS so they can be excluded from future reports. Please refer to Appendix A for an illustration of the breakdown of vulnerability occurrences over time.

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

Table 1: Number of Vulnerabilities by Severity Level

Additionally, the top five high-risk hosts and top five vulnerabilities are displayed in Figure 1.

Vulnerabilities

Figure 1: Top Five High-Risk Hosts

Figure 2: Top Five Risk Based Vulnerabilities

The top five operating systems, services, and vulnerabilities discovered are displayed in Figure 3, Figure 4, and Figure 5 respectively.

Figure 3: Top Five Operating Systems Detected

For Official Use Only (FOUO) 5

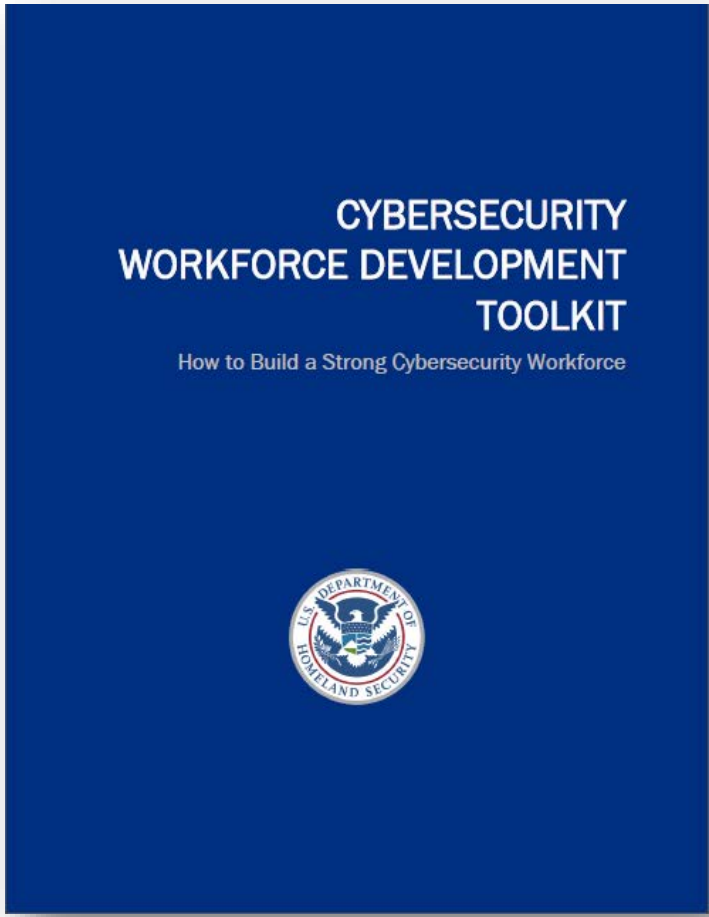
Homeland Security

FINAL THOUGHTS

Creating a Strong Cybersecurity Team

The Cybersecurity Workforce Development Toolkit equips you with resources to:

- ✓ **PREPARE** for workforce development
- ✓ **PLAN** your cybersecurity workforce
- ✓ **BUILD** a high-performing cybersecurity team
- ✓ **ADVANCE** cybersecurity staff with career development opportunities



Available online at niccs.us-cert.gov/

The Foundation for our Nation's Cyber Workforce

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

- ✓ When used nationally, the definitions can help establish universally-applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks

Operate & Maintain | **Securely Provision** | **Analyze** | **Collect & Operate** | **Oversight & Development** | **Protect & Defend** | **Investigate**

Final Thoughts – 1: Know the Planning Considerations

- Strategies: Containment, Eradication, Recovery, Reconstitution, etc
- Incident Categories and Types: Service Disruption, Major / Minor Incident, Data Spill or Breach, Data Exfiltration, Integrity Compromise, Account Compromise, etc
- CSIRT Team and Individual Roles / Responsibilities
  - Authorities to Act (e.g., Seize Equipment, Terminate Services, etc)
  - Authorizations to Communicate to Internal / External Parties
  - Scope of Internal / External Coordination
  - (Secure) Communications
  - Incident Tracking and Status
  - Technical and Analytical Skills and Needs (i.e., live-analysis, network forensics, etc)
  - Knowledge of the Information Technology Infrastructure: Current threats, vulnerabilities, security controls, system configurations, etc.

Final Thoughts – 2: Plan for Partnership

Build external “partnerships” into your incident response plans and allow them a role in your response

Partners	Push / Pull / Poll	Examples
Voluntary Reporting	What happened (impacts and outcomes), when, how, how long, and by whom…	• FBI Internet Crime Compliant Center (IC3) • Fusion Centers (some) • Regional Task Forces (some)
Non-Technical Incident Handling	What you need to know about threat actors, vulnerabilities, etc…	• Fusion Centers (like PA-CIC, DVIC, R13FC) • Regional Task Forces (some) • Information Sharing & Analysis Centers (ISACs)
Technical Incident Response and Assistance	What actions to take, what technical assistance you need…	• DHS ICS-CERT • DHS US-CERT • ISACs (some)
Law Enforcement and Intelligence	Who are the actors, what information or monies can be recovered…	• FBI • USSS • State and Local Police

Final Thoughts - 3:
Resilience Starts with Good Hygiene

Review Layers of Defense:

- Human: → **Policies, Procedures, Training**
- Applications: → **Control Systems, Databases**
- Operating Systems: → **Patch Management, Setup**
- Networks: → **Firewalls, Detection Systems**
- Physical: → **Guards, Gates, Surveillance, Lighting**

- Review Critical Assets and Important Services
- Identify Security and Business Continuity Requirements
- Map Requirements to Security Standards
- Apply Risk-Based Solutions
- Monitor, Monitor, Monitor… (Lather, Rinse, Repeat…)
- Work with your community-of-interest and other resources

Contact Information

Incident Response and Information Sharing
ncciccustomerservice@hq.dhs.gov
General Inquiries
cyberadvisor@hq.dhs.gov
Contact Information

Ronald Watters Cybersecurity Advisor Region X Seattle, WA	Ronald.watters@hq.dhs.gov

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