Critical Cybersecurity Questions

- How do you measure successful cybersecurity efforts?
- Who is accountable for cybersecurity?
- What’s at risk?
- Have you identified the potential consequences if your systems are compromised?
- Have you planned for cyber incident management and exercised that plan?
- Can you sustain operations of critical processes following a significant cyber incident?
- How do these questions apply to your organization?
Cyber Security Framework

Framework Functions

<table>
<thead>
<tr>
<th>Functions</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify</td>
<td>What processes and assets need protection?</td>
</tr>
<tr>
<td>Protect</td>
<td>How are we protecting our networks and data?</td>
</tr>
<tr>
<td>Detect</td>
<td>What are our capabilities for detecting a cyber attack?</td>
</tr>
<tr>
<td>Respond</td>
<td>What are our capabilities for responding to an attack?</td>
</tr>
<tr>
<td>Recover</td>
<td>What are our capabilities for returning to normal operations?</td>
</tr>
</tbody>
</table>
Summary of DHS Cyber Security Offerings

- Cyber Security Advisors
- Protective Security Advisors
- National Cybersecurity and Communications Integration Center (NCCIC)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Preparedness Activities
  - National Cyber Awareness System
  - Stop.Think.Connect
  - Vulnerability Notes Database
  - Technical Threat Indicators
  - Cybersecurity Training
  - Information Products and Recommended Practices
  - National Initiative for Cybersecurity Careers
  - Federal Virtual Training Environment (FedVTE)
  - Cyber Exercise Program
  - Homeland Security Information Network (HSIN)
  - Automated Information Sharing
  - Continuous Diagnostic and Mitigation Program
- National Cybersecurity Assessments and Technical Services (NCATS) Evaluations
  - Cyber Security Evaluation Tool (CSET)
  - Validated Architecture Design Review (VADR)
  - Cyber Hygiene Service (CyHy)
  - Phishing Campaign Assessment (PCA)
  - Risk and Vulnerability Assessment (RVA)
  - Hunt/HIRT (Remote/On-Site Assistance)
  - Malware Analysis
- CSA Facilitated Cyber Security Evaluations
  - Cyber Resilience Review (CRR)
  - Cyber Infrastructure Survey (CIS)
  - External Dependencies Management (EDM) Assessment
- PSA Facilitated Security Evaluations
  - Active Shooter Training
  - Informal Security Walkthrough
  - Infrastructure Survey Tool
  - Dependency Survey Tool
  - Infrastructure Visualization Platform
  - Multi-Asset Security Assessment
NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
  - ncciccustomerservice@hq.dhs.gov

**When to Report:**
If there is a suspected or confirmed cyber attack or incident that:
- Affects core government or critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems;
- Indicates malicious software is present on critical systems

**Malware Submission Process:**
- Please send all submissions to the Advance Malware Analysis Center (AMAC) at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov
# Federal Incident Response

<table>
<thead>
<tr>
<th>Threat Response</th>
<th>Asset Response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Federal Bureau of Investigation (FBI):</strong></td>
<td><strong>United States Computer Emergency Readiness Team:</strong> <a href="http://www.us-cert.gov">http://www.us-cert.gov</a></td>
</tr>
<tr>
<td>FBI Field Office Cyber Task Forces: <a href="http://www.fbi.gov/contactus/field">http://www.fbi.gov/contactus/field</a></td>
<td>Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.</td>
</tr>
<tr>
<td>• Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces.</td>
<td>• Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to the FBI Field Office Cyber Task Forces.</td>
</tr>
<tr>
<td>• Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.</td>
<td></td>
</tr>
<tr>
<td><strong>National Cyber Investigative Joint Task Force (NCIJTF)</strong></td>
<td><strong>The Multi-State Information Sharing and Analysis Center (MS-ISAC)</strong> is a voluntary and collaborative effort designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation’s State, Local, Tribal, and Territorial governments.</td>
</tr>
<tr>
<td>CyWatch 24/7 Command Center:</td>
<td><a href="mailto:soc@msisac.org">soc@msisac.org</a></td>
</tr>
<tr>
<td><a href="mailto:cywatch@ic.fbi.gov">cywatch@ic.fbi.gov</a> or (855) 292-3937</td>
<td></td>
</tr>
<tr>
<td>• Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of Federal law enforcement agencies or the Federal Government.</td>
<td></td>
</tr>
<tr>
<td><strong>United States Secret Service (USSS)</strong></td>
<td><strong>Center for Internet Security (CIS)</strong></td>
</tr>
<tr>
<td>Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): <a href="http://www.secretservice.gov/contact/field-offices">http://www.secretservice.gov/contact/field-offices</a></td>
<td>• Albert Sensors (Intrusion Detection)</td>
</tr>
<tr>
<td><a href="http://www.secretservice.gov/contact/field-offices">http://www.secretservice.gov/contact/field-offices</a></td>
<td>• Vulnerability Management</td>
</tr>
<tr>
<td>• Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.</td>
<td>• Baseline Configuration Guides</td>
</tr>
<tr>
<td><strong>National Cybersecurity and Communications Integration Center (NCCIC)</strong></td>
<td>• Assessment Tools</td>
</tr>
<tr>
<td>(888) 282-0870 or <a href="mailto:NCCIC@hq.dhs.gov">NCCIC@hq.dhs.gov</a></td>
<td></td>
</tr>
</tbody>
</table>
Questions / Discussion?

- Web Resources and Contact CheatSheet:
  - ICS-Cert:
    - https://ics-cert.us-cert.gov/
  - Stakeholder Engagement and Cyber Infrastructure Resilience
  - National Cybersecurity and Communications Integration Center
  - Stop.Think.Connect
    - https://www.dhs.gov/stophinkconnect
  - Critical Infrastructure Cyber Community Voluntary Program (C3VP)
    - https://www.us-cert.gov/ccubedvp
  - Federal Virtual Training Environment
    - https://fedvte.usalearning.gov/
Geoffrey F. Jenista, CISSP  
Cybersecurity Advisor  
Region 7, (NE, IA, MO, KS)  
(913) 249-1539  
geoffrey.jenista@hq.dhs.gov

Harley D. Rinerson  
Chief of Operations - Central  
Cybersecurity Advisor Region 8,  
(CO, UT, WY, SD, ND, MT)  
(202) 809-3314  
Harley.rinerson@hq.dhs.gov

Joseph “JD” Henry  
Cybersecurity Advisor  
Region 7, (NE, IA, MO, KS)  
(202) 860-7546  
Joseph.henry@hq.dhs.gov

For inquiries or further information, contact cyberadvisor@hq.dhs.gov
THE CYBERSECURITY AND INFRASTRUCTURE AGENCY’S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBERSECURITY ASSISTANCE ON A VOLUNTARY, NO-COST BASIS TO CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS. THROUGH THE CSA PROGRAM, YOUR ORGANIZATION CAN PREPARE FOR AND PROTECT AGAINST CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE.

GOALS
The goal of the CSA program is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure, as well as SLTT bodies, through stakeholder partnerships and direct assistance activities.

APPROACH
The CSA program maintains regional subject matter experts throughout DHS emergency management and protection regions. Regional CSAs cultivate partnerships with participating organizations and initiate information sharing. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership. CSAs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the United States.

<table>
<thead>
<tr>
<th>Service</th>
<th>What CSAs Offer</th>
<th>What Value Our Partners Receive</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cyber Preparedness</td>
<td>On-site preparedness and protective visits, workshops, and engaging activities</td>
<td>Cybersecurity ideas, advice, and best practices and a formal exchange to raise awareness of DHS cybersecurity products, services, and information resources relative to critical infrastructure and partnerships</td>
</tr>
<tr>
<td>Strategic Messaging</td>
<td>DHS cybersecurity briefings, keynote addresses, and panel discussions</td>
<td>Improved cybersecurity awareness and collaboration potential, to convey timely and relevant information on DHS programs and operational activities</td>
</tr>
<tr>
<td>Working Group Support</td>
<td>Leadership at existing forums and working groups, engaging stakeholders in-place cybersecurity initiatives and information sharing groups</td>
<td>Improved coordination with DHS on cybersecurity policy, procedures, and best practices; and an opportunity to exchange lessons-learned and identify areas of mutual interest</td>
</tr>
<tr>
<td>Partnership Development</td>
<td>Engagements to develop, build capacity in, and strengthen private-public cybersecurity partnerships</td>
<td>Help initiating cybersecurity partnerships, establishing charter objectives and milestones, and maturing local and regional cybersecurity posture — in order to move partnerships from awareness building to operational capabilities</td>
</tr>
<tr>
<td>Cyber Assessments</td>
<td>Cyber Infrastructure Survey (CIS)</td>
<td>Assessment of more than 80 cybersecurity controls in five domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies, resulting in an interactive decision support tool</td>
</tr>
<tr>
<td>---------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Cyber Resilience Review (CRR)</td>
<td></td>
<td>Assessment of cybersecurity management capabilities and maturity aspects of an organization’s critical information technology (IT) services and associated assets — and in the context of the NIST Cybersecurity Framework (CSF)</td>
</tr>
<tr>
<td>External Dependency Management (EDM)</td>
<td></td>
<td>Assessments of management activities and practices used to identify, analyze, and reduce risks arising from third parties</td>
</tr>
<tr>
<td>Incident Coordination and Support</td>
<td>Direct assistance and resourcing support, conducted in times of cyber threat, disruption, and attack</td>
<td>Facilitated cyber incident response and resource coordination, information de-confliction, and information request assistance</td>
</tr>
</tbody>
</table>

![Cybersecurity Advisors (CSA) Locations](image)

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