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?

Framework Functions

Functions	
Identify	What processes and assets need protection?
Protect	How are we protecting our networks and data?
Detect	What are our capabilities for detecting a cyber attack?
Respond	What are our capabilities for responding to an attack?
Recover	What are our capabilities for returning to normal operations?

Summary of DHS Cyber Security Offerings

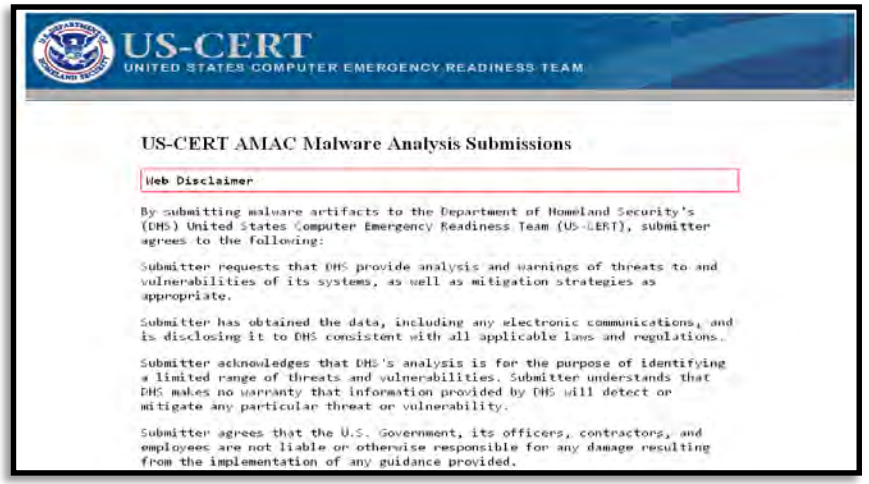
- Cyber Security Advisors
- Protective Security Advisors
- National Cybersecurity and Communications Integration Center (NCCIC)
- Multi-State Information Sharing and Analysis Center (MS-ISAC)
- Preparedness Activities
  - National Cyber Awareness System
  - Stop.Think.Connect
  - Vulnerability Notes 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

Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
  - nccicustomerservice@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

Threat Response	Asset Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contactus/field Internet Crime Complaint Center (IC3): http://www.ic3.gov ▪ 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. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	**United States Computer Emergency Readiness Team:** http://www.us-cert.gov ▪ 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.
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937 ▪ 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.	**The Multi-State Information Sharing and Analysis Center (MS-ISAC)** 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. **1.866.787.4722** **soc@msisac.org**
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.	**Center for Internet Security (CIS)** • Albert Sensors (Intrusion Detection) • Vulnerability Management • Baseline Configuration Guides • Assessment Tools
National Cybersecurity and Communications Integration Center (NCCIC) (888) 282-0870 or NCCIC@hq.dhs.gov	

Questions / Discussion?

- Web Resources and Contact CheatSheet:
  - ICS-Cert:

    https://ics-cert.us-cert.gov/
  - Stakeholder Engagement and Cyber Infrastructure Resilience

    http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience
  - National Cybersecurity and Communications Integration Center

    https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
  - Stop.Think.Connect

    https://www.dhs.gov/stopthinkconnect
  - Critical Infrastructure Cyber Community Voluntary Program (C3VP)

    https://www.us-cert.gov/ccubedvp
  - Federal Virtual Training Environment

    https://fedvte.usalearning.gov/

Contact Information

Geoffrey F. Jenista, CISSP
Cybersecurity Advisor
Region 7, (NE, IA, MO, KS)
(913) 249-1539
geoffrey.jenista@hq.dhs.gov

Joseph "JD" Henry
Cybersecurity Advisor
Region 7, (NE, IA, MO, KS)
(202) 860-7546
Joseph.henry@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

For inquiries or further information,
contact cyberadvisor@dhs.gov

Homeland Security