Homeland Security

Cybersecurity Advisor Program

Geoffrey F. Jenista, CISSP, MBA, MA-ITM
Cybersecurity Advisor (CSA)
Region 7, (NE, IA, MO, KS)
Cybersecurity and Infrastructure Security Agency
(913) 249-1539
geoffrey.jenista@hq.dhs.gov

DHS Cyber Resilience

CYBER SECURITY FRAMEWORK

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 detecting a cyber attack?
Recover What are our capabilities for returning to normal operations?

Critical Cybersecurity Questions:

1. **How do you measure successful cybersecurity efforts?**
2. **Who is accountable for cybersecurity?**
3. **What's at risk?**
4. **Have you identified the potential consequences if your systems are compromised?**
5. **Have you planned for cyber incident management and exercised that plan?**
6. **Can you sustain operations of critical processes following a significant cyber incident?**
7. **How do these questions apply to your organization?**

DHS Cyber Security Assessment Offerings:

National Cybersecurity and Communications Integration Center (NCCIC)

- **National Computer Emergency Response Team (CERT)**
  - **Remote / On-Site Assistance**
  - **Malware Analysis**
- **Cyber Exercise Program**

Preparedness Activities

- **National Cyber Awareness System**
- **Vulnerability Notes Database**
- **Technical Threat Indicators**
- **Cybersecurity Training**
- **Information Products and Recommended Practices**

National Cybersecurity Assessments and Technical Services (NCATS) Assessments

- **Cyber Security Evaluation Tool (CSET)**
- **Validated Architecture Design Review (VADR)**
- **Cyber Hygiene Service**
- **Risk and Vulnerability Assessment (aka "Pen" Test)**
- **Hunt/HIRT**
- **Phishing Campaign Assessment**

CSA Facilitated Cyber Security Assessments

- **Cyber Resilience Review (CRR)**
- **Cyber Infrastructure Survey (CIS)**
- **External Dependencies Management (EDM) Assessment**

Geoffrey F. Jenista, CISSP, MBA, MA-ITM
Cybersecurity Advisor (CSA)
Region 7, (NE, IA, MO, KS)
Cybersecurity and Infrastructure Security Agency
(913) 249-1539
geoffrey.jenista@hq.dhs.gov

Resources

Plan and Build Cyber Resilience Capabilities
National Institute of Standards and Technology (NIST) 800-Series Special Publications The NIST Special Publication (SP) 800 Series comprises information technology security-related publications addressing the NIST Information Technology Laboratory's research, guidelines, and outreach efforts in computer security and its collaborative activities with industry, government, and academic organizations. http://csrc.nist.gov/publications/PubsSPs.html
Critical Infrastructure Cyber Community (C3) Voluntary Program The Department of Homeland Security (DHS) launched the C^3 Voluntary Program in February 2014 to complement the launch of the NIST CSF. The C^3 Voluntary Program helps sectors and organizations that want to use the CSF by connecting them to existing cyber risk management capabilities provided by DHS, other U.S. Government organizations, and the private sector. The C^3 Voluntary Program website describes the various programs DHS offers to critical infrastructure partners, including federal, state, local, and private sector organizations. The CRR self-assessment tool is available on the website or a facilitated assessment contact is provided. www.us-cert.gov/ccubedvp
Department of Homeland Security (DHS) Cybersecurity DHS works across the federal government, partnering with the private sector and empowering the general public to create a safe, secure, and resilient cyber environment, and to +promote cybersecurity knowledge and innovation. https://www.dhs.gov/topic/cybersecurity https://www.dhs.gov/stopthinkconnect
Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) DISA IASE offers products, training, and tools. http://iase.disa.mil/ http://iase.disa.mil/stigs/Pages/index.aspx
CERT Resilience Management Model (CERT-RMM) CERT-RMM is a capability model for operational resilience management that has two primary objectives: (1) Establish the convergence of operational risk and resilience management activities such as security, business continuity, and aspects of IT operations management, into a single model, and (2) Apply a process improvement approach to operational resilience management through the definition and application of a capability level scale that expresses increasing levels of process improvement. www.cert.org/resilience/rmm.html

Cyber Security Evaluation Tool (CSET)
CSET is a standalone DHS tool designed for self-assessment using recognized standards and integrating cybersecurity into an existing corporate risk management strategy. One of the great hidden gems in CSET is the resource library that includes nearly all the available documents produced by the DHS program. It also includes a variety of publicly available documents from NIST and other government sources.

www.us-cert.gov/control_systems/csetdownload.html

Operating in a Cyber Resilient Environment

United States Computer Emergency Readiness Team (US-CERT)
US-CERT is part of the National Cybersecurity and Communications Integration Center NCCIC) at DHS. US-CERT's critical mission activities include the following:

- providing cybersecurity protection to federal civilian executive branch agencies through intrusion detection and prevention capabilities
- developing timely and actionable information for distribution to federal departments and agencies; state, local, tribal, and territorial (SLTT) governments; critical infrastructure owners and operators; private industry; and international organizations
- responding to incidents and analyzing data about emerging cyber threats
- collaborating with foreign governments and international entities to enhance the nation's cybersecurity posture

www.us-cert.gov
www.us-cert.gov/ncas

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
ICS-CERT is part of the National Cybersecurity and Communications Integration Center NCCIC) at DHS. NCCIC/ICS-CERT assists control systems vendors and asset owners/operators to identify security vulnerabilities and develop sound mitigation strategies that strengthen their cybersecurity posture and reduce risk.

www.us-cert.gov/control_systems/ics-cert/
https://ics-cert.us-cert.gov/Training-Available-Through-ICS-CERT
https://ics-cert.us-cert.gov/Assessments

National Cybersecurity and Communications Integration Center (NCCIC)
The NCCIC is responsible for producing a common operating picture for cyber and communications across federal, state, and local governments; intelligence and law enforcement communities; and the private sector.

www.dhs.gov/about-national-cybersecurity-communications-integration-center

Daily Open Source Infrastructure Report
This report, compiled by DHS each business day, summarizes open-source published information concerning significant critical infrastructure issues.

www.dhs.gov/files/programs/editorial_0542.shtm

Homeland Security Information Network (HSIN)
HSIN is a national, secure and trusted portal used for collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission.

www.dhs.gov/files/programs/gc_1156888108137.shtm

Multi-State Information Sharing and Analysis Center (MS-ISAC)
The MS-ISAC is the focal point for cyber threat prevention, protection, response, and recovery for the nation's state, local, territorial, and tribal (SLTT) governments.

https://msisac.cisecurity.org/

Operating in a Cyber Resilient Environment
United State Secret Service (USSS) Electronic Crimes Task Force (ECTF) The USSS/ECTF is a partnership of academia, the private sector and local, state, and federal law enforcement. Its purpose is to prevent, detect, and investigate electronic crimes, including potential terrorist attacks against critical infrastructure and financial payment systems. www.secretservice.gov/investigation/
Federal Bureau of Investigation (FBI) InfraGard InfraGard, a partnership between the FBI and the private sector, is an information-sharing and analysis effort that combines the knowledge base of a wide range of members. https://www.infragard.org/
Internet Crime Complaint Center (IC3) The IC3 is a partnership between the FBI and the National White Collar Crime Center (NW3C). The IC3 is a resource for Internet crime victims to report crimes and alert appropriate agencies online. It collects, reviews, and refers Internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts. It also identifies current crime trends over the Internet. www.ic3.gov/default.aspx
iGuardian The iGuardian portal is an evolution of eGuardian, the platform through which the FBI's law enforcement partners provide potential terrorism-related threats and suspicious activity reports. While eGuardian enlists law enforcement users, iGuardian was developed specifically for partners within critical telecommunications, defense, banking and finance, and energy infrastructure sectors and is available over the sensitive, but unclassified, InfraGard network. https://www.fbi.gov/resources/law-enforcement/iguardian
Research and Education Networking Informatin Sharing and Analysis Center (REN-ISAC) Aids and promotes cybersecurity operational protection and response within the higher education and research (R&E) communities, within the context of a private community of trusted representatives at member institutions, and in service to the R&E community at-large. http://www.ren-isac.net/
Federal Virtual Training Environment (FedVTE) Provides free online cybersecurity training to U.S. government employees, Federal contractors, SLTT, and veterans. https://fedvte.usalearning.gov/