Homeland Security

Helping Your Agency Workforce Prepare for the Next Wave of Cyber Attacks

Federal Network Resilience Division

March 14, 2018

Why Is Training and Awareness so Important?

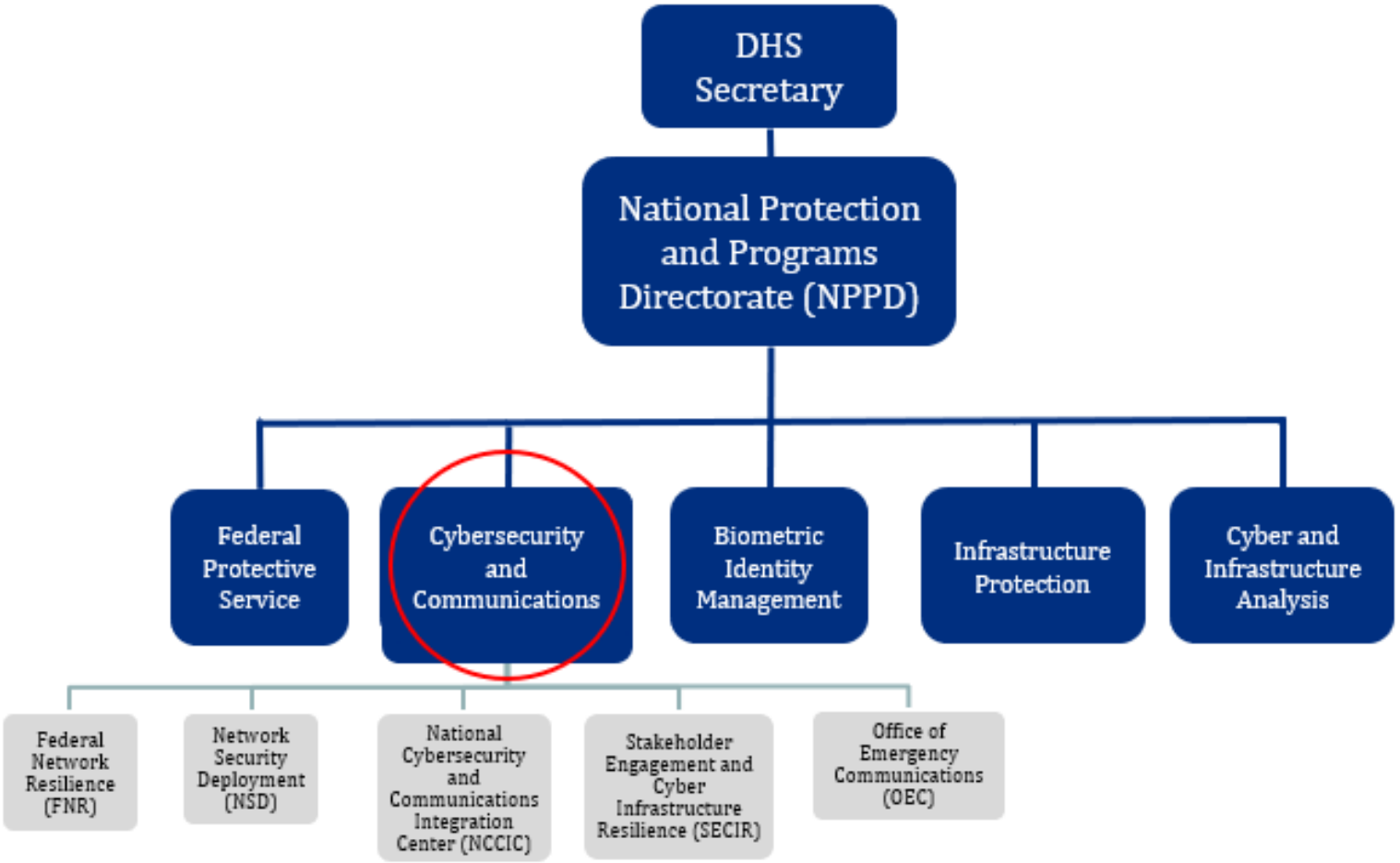
- Technologies and threats are rapidly evolving
- Attacks are more frequent and more sophisticated
- Federal networks and systems are complex, technologically diverse, and geographically dispersed

Key Challenges

- Ensuring security personnel have appropriate skills (*Opportunities Exist to Improve Roles and Address Challenges to Authority,* GAO-16-686, 2016)
- Identifying and closing skills gaps (*Federal Efforts Are Under Way That May Address Workforce Challenges*, GAO-17-533T, 2017)

We have to keep up to protect our systems and data!

Office of Cybersecurity and Communications (CS&C) Mission Space



CS&C Training and Awareness Resources

CS&C offers a variety of resources to help build cybersecurity knowledge and skills across the Federal Enterprise.

- Technical Assistance and Training
- Analytical Tools and Programs
- Resources and Publications

Technical Assistance and Training

CS&C Provides Technical Assistance and Training on a Variety of Topics:

- Cybersecurity Performance Management
- Risk Assessment and Management
- Governance
- Assurance
- Vulnerability Management
- Incident Response

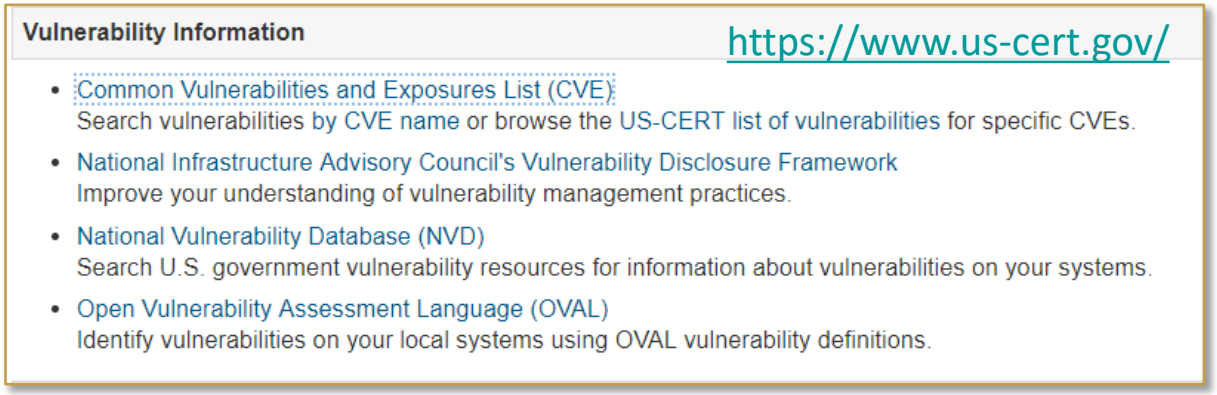
Technical Assistance and Training (cont.)

Examples:

- CDM Capability Training Workshops (e.g., Agency Dashboard training)
- Information Security Continuous Monitoring Training Workshops
- Monthly Cyber Insights Webinar Series
- Federal Virtual Training Environment (FedVTE)
  - https://fedvte.usalearning.gov/
- Risk and Vulnerability Assessments
- Architecture Design Reviews
- High Value Asset Assessments

Analytical Tools and Programs

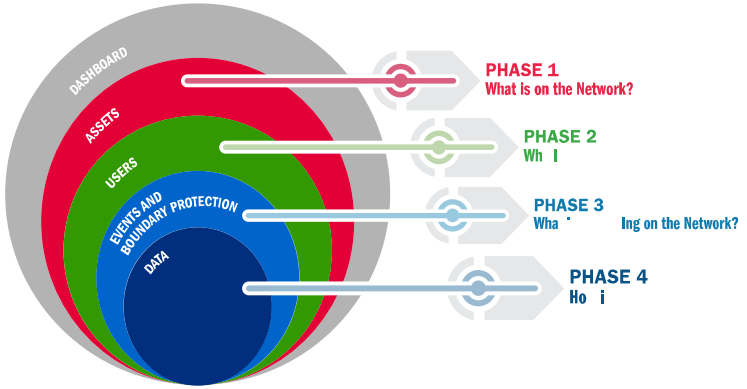
- Federal Incident Notification Guidelines
- National Cybersecurity Protection System (NCPS) and EINSTEIN Program
- Information Sharing Programs
  - Automated Indicator Sharing (AIS)
  - Cyber Information Sharing and Collaboration Program (CISCP)
- Vulnerability Knowledge Database



Analytical Tools and Programs (cont.)

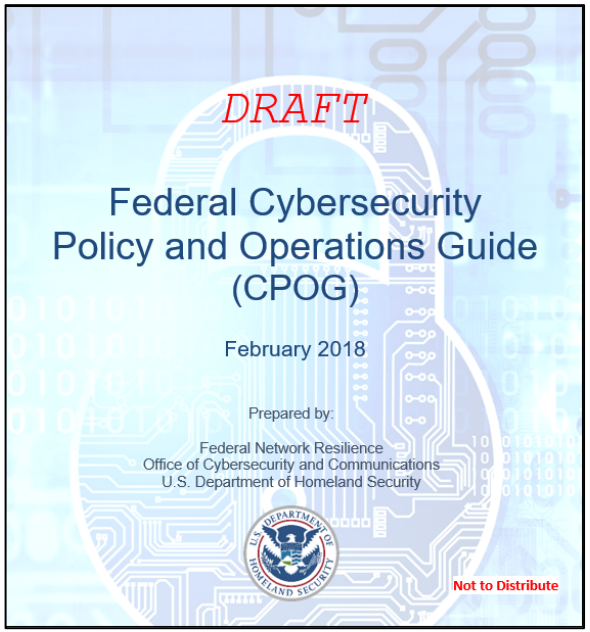
Continuous Diagnostics and Mitigation (CDM)

- The CDM Program enables federal agencies to expand their network sensor capacity and automate cybersecurity testing and validation, and prioritize risks
- There are multiple interagency working groups to enhance understanding and implementation
  - Customer Advisory Forum (CAF) – Focal point for CDM coordination and collaboration
  - Ongoing Authorization Working Group (OAWG) – Charged with identifying best practices
  - Risk Integrated Project Team (RIPT) – Focused on risk scoring
- CDM Agency Dashboard training to help analysts maximize its use



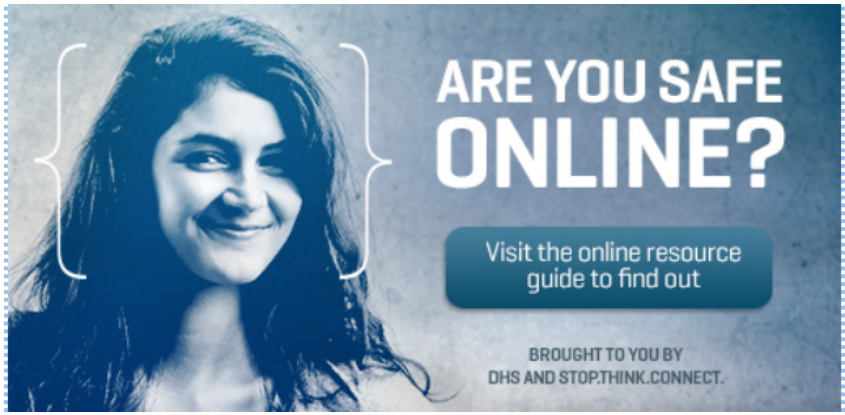
Resources and Publications

- Technical Documents
  - Basics of Cloud Computing
  - System Integrity Best Practices
  - Cyber Threats to Mobile Devices
- Fact Sheets
  - Anonymous Networks and Currencies
  - Insider Threat
  - Mobile Device Security
- Cybersecurity Governance Toolkit (coming soon!)
- Cybersecurity Policy Operational Guide (CPOG) (coming soon!)



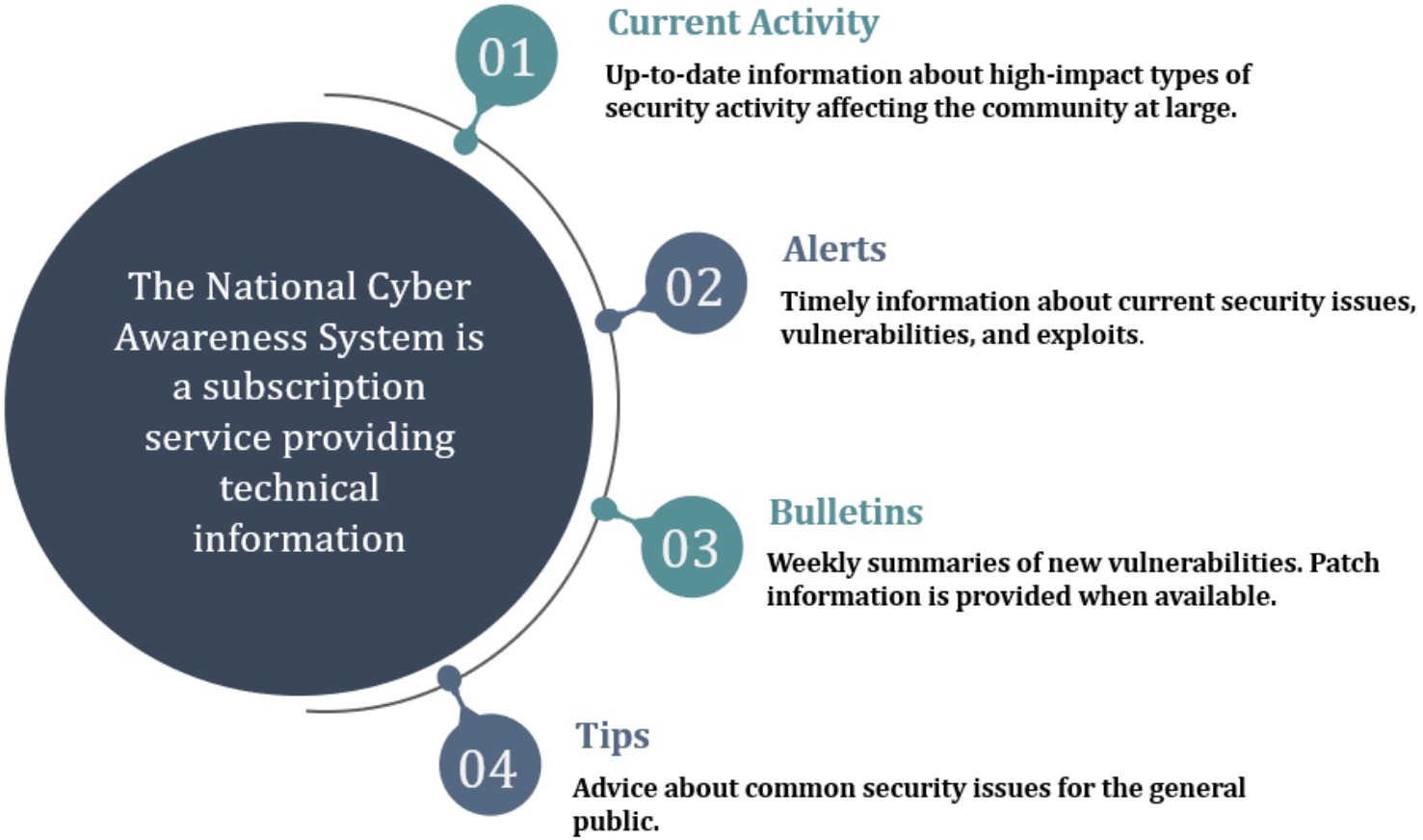
Resources and Publications (cont.)

- "Build Security In Website
  - Collaborative effort to build security into software development
  - Best practices and lessons learned
  - Explanations of security tools
- Stop.Think.Connect
  - National public awareness campaign
    - Increases the understanding of cyber threats
    - Empowers the American public to be safer and more secure online
  - Toolkit, blog, video series



Build Security In: https://www.us-cert.gov/bsi
Stop.Think.Connect: https://www.dhs.gov/stopthinkconnect

Keeping up with Cybersecurity Trends and Info



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

Collaboration with Other Stakeholders

Stakeholder	Resource Description and Link
Federal CIO Council	The principal interagency forum for improving agency practices related to the design, acquisition, development, modernization, use, sharing, and performance of Federal information resources https://www.cio.gov/
Government Forum of Incident Response and Security Teams (GFIRST)	A group of technical and tactical practitioners of security response teams responsible for securing government information technology (IT) systems https://www.us-cert.gov/government-users/collaboration/gfirst
Information Technology-Information Sharing and Analysis Center (IT-ISAC)	A non-profit, limited liability corporation formed by members of the IT sector as a forum for managing risks and IT infrastructure. This is part of the larger ISAC community to encourage information sharing between different sectors. https://www.it-isac.org/

CS&C Is Ready and Willing to Help

- CS&C resources are already developed to help increase cybersecurity knowledge
  - Helps ensure security personnel have appropriate skills
  - Helps identify and close skill gaps
- CS&C resources help agencies improve security posture and meet Federal requirements
- CS&C resources support the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework Cybersecurity Framework

Let Us Help!

Alexis Wales
Federal Network Resilience Division
Office of Cybersecurity and Communications
Alexis.Wales@HQ.DHS.GOV