Cyber Resilience Workshop
Participant Handout

Definition of *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

Key components of cyber resilience

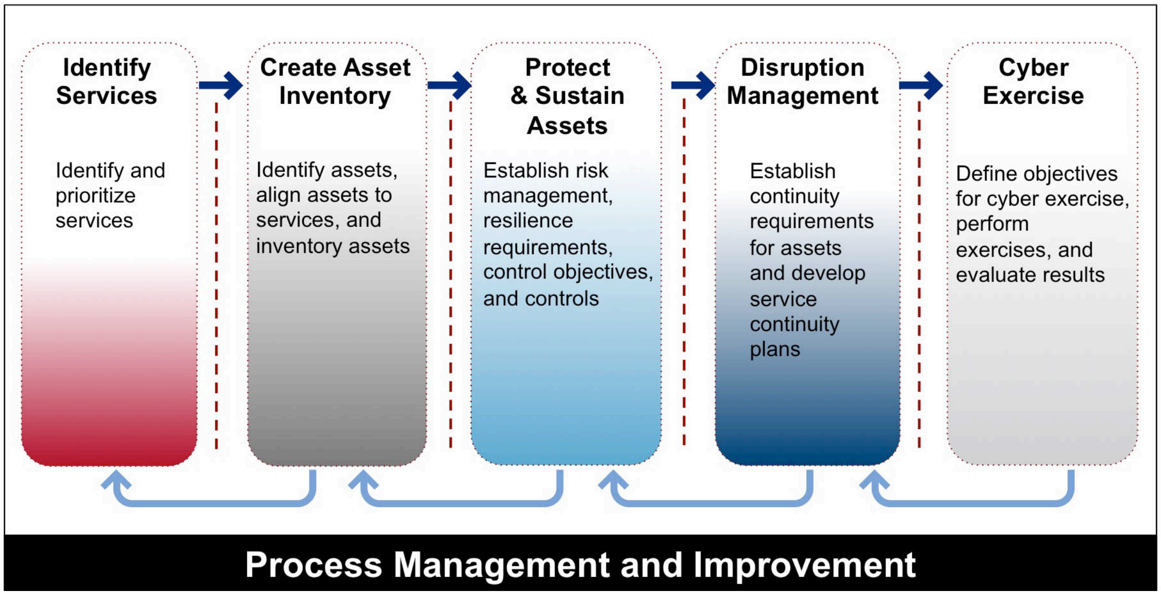
Survivability

- is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures (including large-scale natural disasters)

Disruption tolerance

- is the ability for selected functions to continue to operate even when the supporting infrastructure is not operating at an optimum level
- allows an organization to more realistically assess its operational risks and make strategic decisions for continuation of operations in the face of natural or man-made challenges

Cyber resilience approach


Identify Services
Identify and prioritize services
Create Asset Inventory
Identify assets, align assets to services, and inventory assets
Protect & Sustain Assets
Establish risk management, resilience requirements, control objectives, and controls
Disruption Management
Establish continuity requirements for assets and develop service continuity plans
Cyber Exercise
Define objectives for cyber exercise, perform exercises, and evaluate results
Process Management and Improvement

Because this approach is built on process management and improvement

- having robust and fully implemented processes is critical
- these processes support the activities of operational resilience
- the practices put in place can be sustained and will continue even in a crisis situation

Without this level of organizational discipline, an organization's operational resilience is only as good as the efforts of its employees.

Cyber Resilience Workshop
Participant Handout

Identify Services and Manage Their Assets

- ☐ Identify services
- ☐ Prioritize services
- ☐ Identify assets
- ☐ Align assets to services
- ☐ Inventory assets
- ☐ Cyber resilience processes that rely on an asset inventory

Protect and Sustain

- ☐ Cyber resilience and operational risk management
- ☐ Identify cyber resilience requirements for services
- ☐ Use cyber resilience requirements to develop control objectives and controls
- ☐ Use control objectives to evaluate the performance of a cyber resilience management program

Cyber Resilience Workshop
Participant Handout

Managing Business Disruptions: Service Continuity and Incident Management

□ Disruption management overview – Service Continuity and Incident Management

□ Critical role of defining requirements

□ Establish Service Continuity & Incident Management Processes

□ Exercising to promote ongoing validation, improvement and quality

Managing for Cyber Security Success

□ What a successful cybersecurity program looks like

□ How exercises and testing support quality, improvement, and “make it stick” objectives – leveraging what you have

□ How optimizing cybersecurity can be the hard part

□ Efficiency and “making it stick” over the long haul

Cyber Resilience Workshop
Participant Handout

Resources	
Planning and Building Cyber Resilience Capabilities	
NIST 800-Series Special Publications	The NIST Special Publication (SP) 800 Series comprises information technology security-related publications addressing ITL's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations. **NIST 800-Series Special Publications:** http://csrc.nist.gov/publications/PubsSPs.html
Critical Infrastructure Cyber Community (C3)	DHS launched the C3 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 C3 website describes the various programs DHS offers to critical infrastructure partners, including Federal, State, local, and private sector organizations CRR self assessment tool is available on the website or a facilitated assessment contact is provided. http://www.us-cert.gov/ccubedvp
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 promote cybersecurity knowledge and innovation. **Cybersecurity:** http://www.dhs.gov/files/cybersecurity.shtm **Tools, links, tips:** http://www.dhs.gov/stopthinkconnect-get-informed
Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE)	DISA IASE offers products, training, and tools. **DISA IASE:** http://iase.disa.mil/ **DISA Security Technical Implementation Guides (STIGs):** http://iase.disa.mil/stigs/index.html
CERT® Resilience Management Module (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. 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. **CERT-RMM:** http://www.cert.org/resilience/rmm.html
Cyber Security Evaluation Tool (CSET®)	CSET is a stand-alone DHS tool designed for • self-assessment using recognized standards

® CERT is a registered trademark of Carnegie Mellon University.

	• 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. **CSET Download:** 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 the operational arm of the National Cyber Security Division (NCSD) at DHS. US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans. **US-CERT:** http://www.us-cert.gov/ **National Cyber Alert System:** http://www.us-cert.gov/ncas
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)	ICS-CERT provides a control system security focus in collaboration with US-CERT. ICS-CERT serves as a key component of the Strategy for Securing Control Systems, which outlines a long-term, common vision where effective risk management of control systems security can be realized through successful coordination efforts. **ICS-CERT:** http://www.us-cert.gov/control_systems/ics-cert/ **CSSP Training:** http://ics-cert.us-cert.gov/sites/default/files/DHS_CyberSecurity_CSSP-Traning-v12.pdf **Cyber Security Evaluation Tool (CSET):** http://www.us-cert.gov/control_systems/satool.html
National Cybersecurity and Communications Integration Center (NCCIC)	The NCCIC is a 24x7 center responsible for the production of a common operating picture for cyber and communications across the federal, state, and local government, intelligence, and law enforcement communities, and the private sector. **NCCIC:** http://www.dhs.gov/about-national-cybersecurity-communications-integration-center
Daily Open Source Infrastructure Report	Each business day, the DHS collects a summary of open-source published information concerning significant critical infrastructure issues. **Daily Open Source Infrastructure Report:** http://www.dhs.gov/files/programs/editorial_0542.shtm
Homeland Security Information Network (HSIN)	HSIN is a national secure and trusted web-based portal for information sharing and collaboration among federal, state, local, tribal, territorial, private sector, and international partners engaged in the homeland security mission. **HSIN:** http://www.dhs.gov/files/programs/gc_1156888108137.shtm
Multi-State Information Sharing and Analysis Center	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. http://msisac.cisecurity.org/resources/videos/free-training.cfm

Operating in a Cyber Resilient Environment	
United State Secret Service (USSS) Electronic Crimes Task Force (ECTF)	Partnership of not only federal, state, and local law enforcement, but also prosecutors, private industry, and academia. Its common purpose is the prevention, detection, mitigation, and aggressive investigation of attacks on the nation's financial and critical infrastructures. **USSS ECTF:** http://www.secretservice.gov/ectf.shtml
Federal Bureau of Investigation (FBI) InfraGard	InfraGard, a partnership between the FBI and the private sector, is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. **InfraGard:** http://www.infragard.net/
Internet Crime Complaint Center (IC3)	The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). The IC3 • provides a central point for Internet crime victims to report to and alert an appropriate agency online at www.ic3.gov • collects, reviews, and refers Internet crime complaints to law enforcement agencies with jurisdiction to aid in preventive and investigative efforts • identifies current crime trends over the Internet **IC3:** http://www.ic3.gov/default.aspx
iGuardian	The portal, iGuardian, in its pilot stage, is available to 58,000 companies that make up the FBI's InfraGard network. If the pilot succeeds, the FBI plans to open it up to more organizations, probably at first in critical infrastructure sectors. Participating companies can submit a form online in the instance of a cybersecurity breach to their networks. The National Cyber Investigative Joint Taskforce (NCI-JTF) handles the information provided by these companies. **iGuardian:** http://www.fbi.gov/news/podcasts/thisweek/iguardian.mp3/view **NCI-JTF:** http://www.fbi.gov/about-us/investigate/cyber/ncijtf

Cyber Exercise	
DHS National Cyber Security Division, Cyber Exercise Program (NSCD-CEP)	The **NCSD-CEP** improves the nation's cybersecurity readiness, protection, and incident response capabilities by developing, designing, and conducting cyber exercises and workshops at the state, federal, regional, and international level. The NCSD-CEP employs scenario-based exercises that focus on risks to the cyber and information technology infrastructure. **NCSD-CEP:** http://www.us-cert.gov/sites/default/files/publications/infosheet_Cyber%20Exercises.pdf
FEMA IS-139 Exercise Design – National Preparedness Directorate	This course is based on the premise that emergency exercises are worth the effort. Exercises identify areas that are proficient and those that need improvement. The course is designed to introduce the fundamentals of exercise design. **FEMA Indepent Study Course:** www.training.fema.gov/emiweb/IS/is139lst.asp
DHS Homeland Security Exercise Evaluation Program (HSEEP)	The HSEEP doctrine consists of fundamental principles that frame a common approach to exercises. Applying these principles to both the management of an

	exercise program and the execution of individual exercises is critical to the effective examination of capabilities. **DHS – HSEEP:** https://www.llis.dhs.gov/hseep
SANS Penetration Tests and Red Team Exercises	The process and tools used to simulate attacks against a network to validate the overall security of an organization. **SANS:** https://www.sans.org/critical-security-controls/control.php?id=20
ISACA: The Minimum IT Controls to Assess in a Financial Audit	There are certain IT areas, IT general controls (ITGC), that systemically affect almost all financial audits because of their ubiquity and significance. Therefore, these areas could apply to any financial audit client and should be assessed as to their level of applicable risk to the audit objectives in all financial audits. **ISACA:** http://www.isaca.org/Journal/Past-Issues/2010/Volume-1/Pages/The-Minimum-IT-Controls-to-Assess-in-a-Financial-Audit-Part-I-1.aspx
How to Exercise Your Crisis Management Team	An article by Chris MacArthur http://www.continuitycentral.com/feature0978.html
SANS Training Exercises For IT Support Employees	Article by Keil Hubert in the SANS Institute InfoSec Reading Room http://www.sans.org/reading-room/whitepapers/bestprac/practical-cyber-security-training-techniques-support-employees-34267?show=practical-cyber-security-training-techniques-support-employees-34267&cat=bestprac

Contact Information

Bradford Willke	bradford.willke@hq.dhs.gov

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