



ISOAG Meeting

April 5, 2017

Welcome to CESC



Welcome and Opening Remarks

Michael Watson

April 5, 2017



ISOAG April 5, 2017 Agenda

- | | |
|---|-----------------------------|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Managing Cyber Risk, and Improving Cyber Resiliency | Reggie McKinney, DHS & CS&S |
| III. Continuity of Operations Planning | Donna Pletch, VDEM |
| V. Upcoming Events | Mike Watson, VITA |
| VI. Partnership Update | Northrop Grumman |

Cybersecurity Resources

Presented to:

**Virginia Information Technologies Agency
Information Security Officers Advisory Group**

April 5, 2017

Reggie McKinney
C³ Voluntary Program
Office of Cybersecurity and Communications
National Protection and Programs Directorate



Homeland Security

Agenda

- Threat Environment
- Cybersecurity Framework
- DHS Cybersecurity Resources
 - C³VP SLTT tools
 - Office of Cybersecurity and Communications resources



SLTT: State, Local, Tribal, and Territorial governments

Cyber Attacks on the Commonwealth

“We experienced 86 million cyber attacks on our state accounts last year.”

Virginia Governor Terry McAuliffe
New America Conference, March 20, 2017



Attacks on Other State Governments

Hawaii

45 million attacks daily
Honolulu Star Advertiser
(1/12/17)

South Carolina

5 million attempts weekly to access
state computers, including 100,000
weekly virus / malware attacks
Charleston Post Courier
(3/17/17)

Texas

5 billion attacks monthly
Texas Start Telegram
(2/27/17)

Wisconsin

6 million attacks daily
Fox6Now.com
(3/10/15)

These numbers represent attempted infiltrations, not successful attacks.



SLTT Cyber Attack Trends

- Increase in Distributed Denial of Service (DDOS) attacks (flooding networks with data to overwhelm resources)
- Increase in complexity of malware attacks (criminals, nation states, hacktivists)
- Increase in attacks promoting political, social, and ideological causes (hacktivism)
- Increase in damages (in addition to stealing personal information, adversaries are trying to shut down services to extort money)

Source: *2015 Nationwide Cyber Security Review: Summary Report* (DHS in partnership with Multi-State Information Sharing and Analysis Center)

Despite the Growing Threat ...

- Many of the vulnerabilities are well known and fixable
- The cybersecurity community knows how to identify adversaries and thwart attacks before damages occur
- The cybersecurity community also knows how to respond quickly and effectively when incidents occur
- Sound management – coupled with sound technology – can effectively counter the threat





Cybersecurity Framework

Cybersecurity Framework Partnership



- Developed the Framework in concert with stakeholders
- Currently enhancing the Framework (direct comments on draft version 1.1 to cyberframework@nist.gov by April 10th, 2017)
- Supports DHS activities
- Develops Framework Implementation Guidance and other cybersecurity tools
- Conducts educational events and outreach to critical infrastructure sectors, SLTT, and small and medium size businesses (SMBs)
- Supports NIST activities

Cybersecurity Framework Draft Version 1.1
<https://www.nist.gov/cyberframework/draft-version-11>

Cybersecurity Framework Summary

- **Flexible** performance-based approach for identifying, assessing, and managing cyber risk
- **Common language** and systematic methodology
- Applicable to **any size organization** in any sector (including non-critical infrastructure)
- Used by both **sophisticated and starter** cyber risk programs
- Virginia: first state to adopt

Framework for Improving Critical
Infrastructure Cybersecurity

Version 1.0

National Institute of Standards and Technology

February 12, 2014

A Holistic Approach to Cybersecurity

Functions	Categories
Identify	Asset Management
	Business Environment
	Governance
	Risk Assessment
	Risk Management Strategy
Protect	Access Control
	Awareness and Training
	Data Security
	Information Protection Processes & Procedures
	Maintenance
	Protective Technology
Detect	Anomalies and Events
	Security Continuous Monitoring
	Detection Processes
Respond	Response Planning
	Communications
	Analysis
	Mitigation
	Improvements
Recover	Recovery Planning
	Improvements
	Communications

- Five **functions** align to **categories** (and sub-categories, not depicted) that represent key disciplines that need to work together to manage cyber risk
- This holistic approach fosters operational integration and effective communication across the entire organization

The Framework covers the full breadth of cybersecurity.

Note: For a description of Framework Components (Core Functions, Implementation Tiers, and Profiles) visit <https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-virtual-events>

Framework Uses

Use the Framework to ...

- Conduct assessments, identify gaps, determine priorities based on best practices
- Demonstrate the need for resources to leadership
- Communicate needs and expectations across the organization and with vendors using a common vocabulary
- Enhance employee on-boarding and training
- Inform internal policies and vendor requirements



Cybersecurity Resources

C³VP Resources



C³VP website

- ~40 tools and resources to help organizations use the Framework and increase their cybersecurity
- Organized by stakeholder group, including SLTT

C³VP website

<https://www.us-cert.gov/ccubedvp>

SLTT Page

C3 VOLUNTARY PROGRAM

Critical Infrastructure Cyber Community Voluntary Program

- Home
- Cybersecurity Framework
- Academia
- Business
- Federal Government
- Small and Midsize Businesses
- SLTT Government**
- Communications Tools
- Assessments
- Events and Media

Resources for State, Local, Tribal, and Territorial (SLTT) Governments

The resources below are available to State, local, tribal, and territorial governments. Resources have been aligned to the five Cybersecurity Framework Function Areas. Some resources and programs align to more than one Function Area.

At the bottom of this page are links to geographically-specific resources from various levels of government to help identify and manage cyber risk.

C³ Voluntary Program SLTT Toolkit

To help SLTT government leaders get started, DHS has created a packet of resources specially designed to help them recognize and address their cybersecurity risks. Resources include discussion points for government leaders, steps to start evaluating a cybersecurity program, and a list of hands-on resources available to SLTT governments.

1. SLTT Toolkit Table of Contents
2. Begin the Conversation: Understanding the Threat Environment
3. SLTT Government Leadership Agenda
4. Hands-On Resource Guide
5. C³ Voluntary Program FAQs

On This Page:

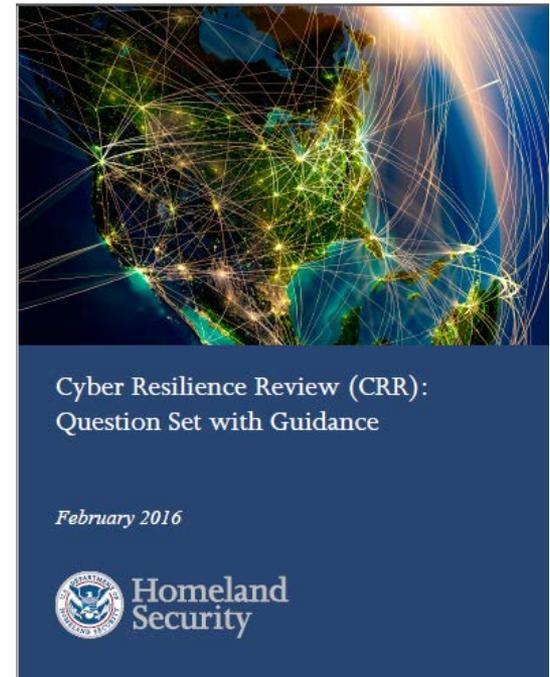
- Identify
- Protect
- Detect
- Respond
- Geographically Specific Resources

A range of cybersecurity resources are aligned to the Framework's five core functions



Cyber Resilience Review (CRR)

- Methodology for evaluating operational resilience and practices across ten foundational cybersecurity domains
- Assesses an organization's security management capabilities and gaps against the NIST Cybersecurity Framework
- Facilitated by DHS or self-administered



DHS Cybersecurity Advisors administer CRRs within their respective regions; they also provide guidance on cybersecurity.

Automated Indicator Sharing (AIS)

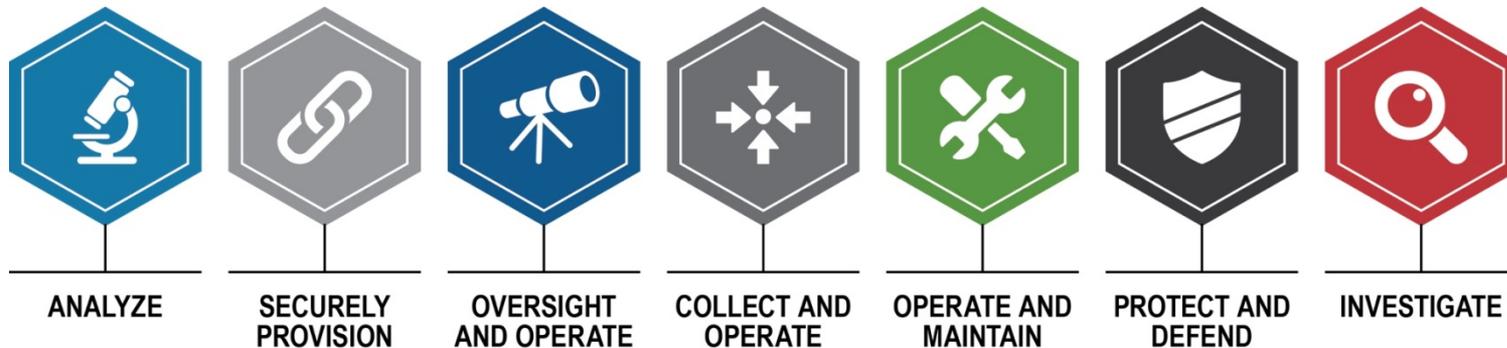
- Enables exchange of cyber threat indicators – such as IP addresses or phishing emails – at machine speed
- Available to private sector entities; federal departments and agencies; SLTT governments; information sharing and analysis centers (ISACs) and information sharing and analysis organizations (ISAOs); and foreign partners and companies
- Participants validate the indicators – this enables DHS to share indicators as quickly as possible
- Participants remain anonymous to the AIS community
- Privacy and civil liberties protections regularly tested

Information sharing is critical to our Nation's cybersecurity.



National Cybersecurity Workforce Framework

- Provides strategies and resources for public or private sector workforce design, professionalization, recruitment, and retention
- Describes cyber positions, tasks, and related knowledge, skills, abilities
- Organizes the work required for a cyber capability



Free Cybersecurity Training: FedVTE

- Online training (**FedVTE**) plus real-time, instructor-led courses (**FedVTE Live!**) serving SLTT employees and U.S. veterans
- 137,000+ active users
- Beginner to advanced courses, including certification preparation for industry exams:
 - Network +
 - Security +
 - Certified Information Systems
 - Security Professional
 - Certified Ethical Hacker



FedVTE
fedvte.usalearning.gov

FedVTE Live!
fedvtelive@hq.dhs.gov

Final Thoughts

- Integrate Framework functions and vocabulary into your day-to-day ISO management activities
- Visit these websites for cybersecurity resources:
 - Cybersecurity Framework webinar: <https://www.nist.gov/news-events/events/2017/03/cybersecurity-framework-virtual-events>
 - C³VP website: <https://www.us-cert.gov/ccubedvp>
 - FedVTE: fedvte.usalearning.gov
 - FedVTE Live!: fedvtelive@hq.dhs.gov





The Commonwealth of Virginia Continuity Planning Program

Introduction and Requirements

- ▶ The Commonwealth first began continuity planning in 2007.
- ▶ *Code of Virginia § 44-146.18*: ...The Virginia Department of Emergency Management shall provide guidance and assistance to state agencies and units of local government in developing and maintaining emergency operations and **continuity of operations programs, plans and systems...**
- ▶ VDEM developed planning guidance and a template, which executive branch agencies and state institutions of higher education are required to follow per Executive Order #41 (2011).

Introduction and Requirements

- ▶ Executive branch agencies and institutions of higher education are required to annually submit a copy of their continuity plan to VDEM by April 1st.
 - ▶ The Secretary of Public Safety and Homeland Security, in collaboration with VDEM, is required to annually report on the status of Commonwealth executive branch agency continuity planning to the Governor by December 31st.
- 

Commonwealth Continuity Planning

- ▶ Functions based planning:
 - Not based on a single facility or group of facilities
 - Not IT centric
 - Considers the functions performed by the entire agency, regardless of the location where they are performed
 - Agencies may elect to have district or division offices develop their own continuity plans, but VDEM only requires one overarching plan that encompasses all agency functions
 - Should be an coordinated agency wide planning effort
 - Should consider three planning scenario's or any combination thereof

All Hazards and Scalable

Planning for disasters and non-disaster disruptions

- ▶ Loss of a facility or a portion of a facility



All Hazards and Scalable

Planning for disasters and non-disaster disruptions

- ▶ Equipment or system failure



All Hazards and Scalable

Planning for disasters and non-disaster disruptions

- ▶ Loss of services due to a reduced workforce



All Hazards and Scalable

Planning for disasters and non-disaster disruptions

- ▶ Can more than one hazard occur at the same time?



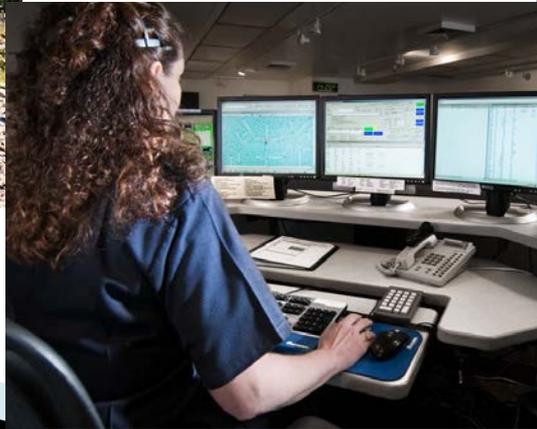
Continuity Plan Core Components

- ▶ Identify Mission Essential Functions:
 - Why was the agency created?
 - What is the agency required to do by law, executive order, or other binding documents.
 - Does the agency provide services that are essential to state or local disaster response and recovery?



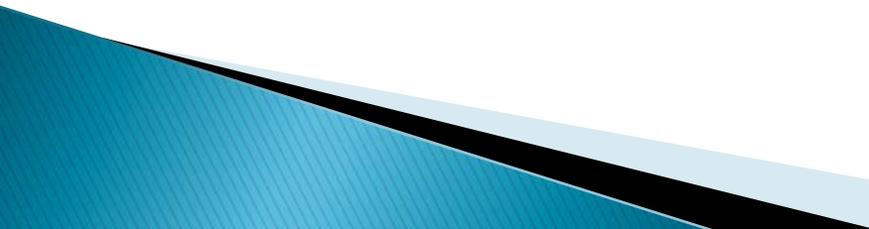
Continuity Plan Core Components

- ▶ Identify supporting Primary Business Functions:
 - Departments and/or divisions document how the function is performed, interdependencies, IT or equipment requirements, staffing requirements, etc.



Continuity Plan Core Components

- ▶ Recovery Time Objectives:
 - Should be identified for all mission essential and primary business functions
 - How long can the agency go without this function being performed?

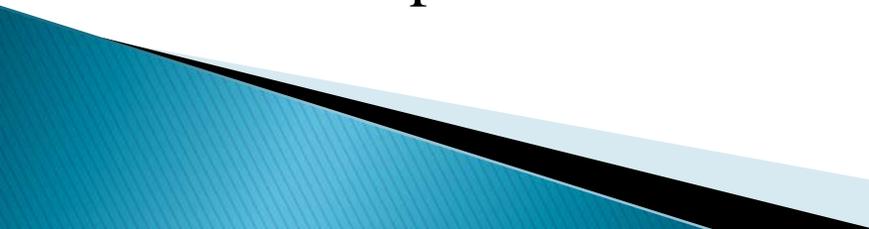
 - ▶ Alternate facility locations:
 - An MOU for use of the facility should be signed and have an expiration date requiring review/renewal
 - Consider telework as an alternative option if staff have the necessary equipment and means to do so
- 

Continuity Plan Core Components

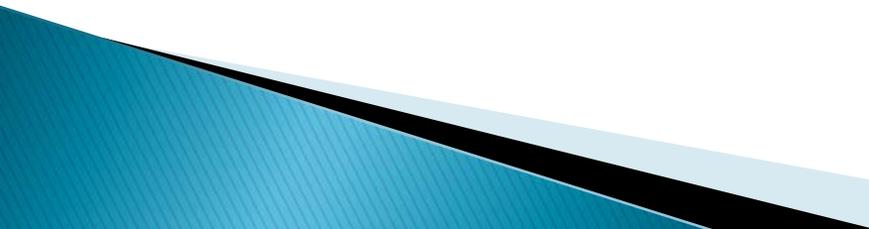
- ▶ **Orders of Succession:**
 - Complete for all leadership (decision-making) positions within the agency
 - Positions identified should have at least two successors

 - ▶ **Delegations of Authority:**
 - Complete for all statutory or signatory authorities
- 

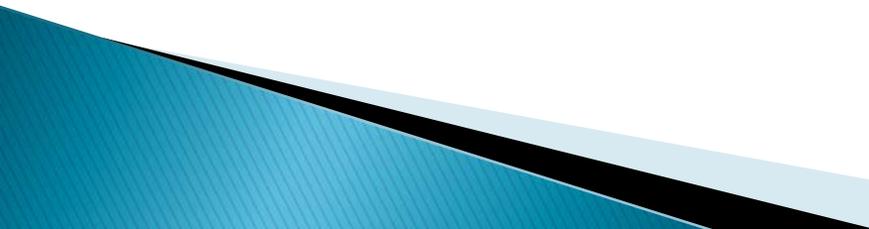
Continuity Plan Activations

- ▶ Over the past several years there have been approximately 10-20 COOP activations by state agencies and institutions of higher education per year.
 - ▶ Majority of activations are due to facility-related impacts (structural or loss of utilities)
 - Fire and sprinkler system activation
 - Water main break
 - Forced relocation due to a special event
 - ▶ In some instances, both the facility and IT infrastructure were impacted
- 

A Sampling of Best Practices

- ▶ Clearly communicating with employees during a COOP activation
 - Are they to report to an alternate work area or telework?
 - What is expected of them?
 - Who is going to make sure they have what they need to work?
 - ▶ Identifying which servers house critical IT applications that support primary business functions and mission essential functions
- 

A Sampling of Best Practices

- ▶ Storing spare vehicle keys at an alternate facility
 - ▶ Capability to remotely auto-forward a critical phone line (24 hour call center) to another phone without going through your service provider
 - ▶ Establishing memorandums of agreement with agencies or organizations that have similar unique needs
- 

VDEM's Continuity Plan Template

- ▶ VDEM's continuity plan template can be found on our web site at:

<http://www.vaemergency.gov/emergency-management-community/emergency-management-plans/continuity-planning/>

Questions?

Donna Pletch
Strategic Planning Branch Chief
Virginia Department of Emergency Management
Donna.Pletch@VDEM.Virginia.gov
(804) 674-2426



Virginia Information Technologies Agency

Upcoming Events





Virginia Information Technologies Agency

(ISC)2 Richmond Metro Chapter meeting will be held on April 27th between 6 pm and 8 pm at John Tyler Community College Midlothian Campus. 800 Charter Colony Parkway, Midlothian VA 23114.



Future ISOAG

May 3, 2017 1:00 - 4:00 pm @ CESC

**Speaker: David Ihrie & Guests,
Center for Innovation Technology**

ISOAG meets the 1st Wednesday of each month in 2017

ADJOURN

THANK YOU FOR ATTENDING

