



STOP | THINK | CONNECT™

# Cyber Security & Homeland Security: Moving Toward Cyber Resilience

5 October 2011

Bradford J. Willke

Mid-Atlantic Cyber Security Advisor  
Cyber Security Evaluation Program (CSEP)  
National Cyber Security Division (NCSD)  
Office of Cyber Security and Communications (CS&C)



Homeland  
Security

# National Cyber Security Division @ DHS

National Cyber Security Division

Federal Network  
Security

Network Security  
Deployment

United States  
Computer  
Emergency  
Readiness Team

Global Cyber  
Security  
Management

Critical  
Infrastructure Cyber  
Protection &  
Awareness



Homeland  
Security

# A Few Recent Cyber Incidents...

<b>January</b>	Canadian Government reports major cyber intrusions at Finance Department and Treasury Board
<b>March</b>	Cryptography firm, RSA, suffered a massive network intrusion that resulted in the theft of information related to its SecurID tokens (45 million)
<b>April</b>	Epsilon, which handles email and market communications for more than 2,500 clients worldwide (7 of the Fortune 10) - exposed millions of customer email addresses
<b>May</b>	Lockheed Martin, Booz Allen Hamilton and other Defense Contractors – networks penetrated by attackers who used RSA tokens (exploit from prior breach)
<b>May</b>	Citibank - 360,000 accounts hacked, exposing names, numbers, and contact information of bank customers
<b>June</b>	Atlanta's FBI InfraGard Chapter - usernames and passwords published online
<b>August</b>	BART website hacked twice, releasing both customers' personal data and personal data for some members of BART police



# Outreach and Awareness

- National Cyber Security Awareness Month (October)
- Nationwide Cyber Security Review (NCSR) for State and Large Urban Area (i.e., UASI) stakeholders
- StaySafeOnline.org
  - Simple, practical steps for:
    - Home computer users
    - K-12 and higher-education environments
    - Small to medium size enterprises



**Homeland  
Security**

# Industrial Control System – Computer Emergency Readiness Team (ICS-CERT)

- Mission objectives
  - Responds to and analyzes control systems related incidents
  - Conducts vulnerability and malware analysis
  - Providing onsite support for forensic investigations
  - Providing situational awareness in the form of actionable intelligence
  - Coordinates the responsible disclosure of vulnerabilities and mitigations
  - Shares and coordinates vulnerability information and threat analysis through information products and alerts
- [http://www.us-cert.gov/control\\_systems/ics-cert/](http://www.us-cert.gov/control_systems/ics-cert/)

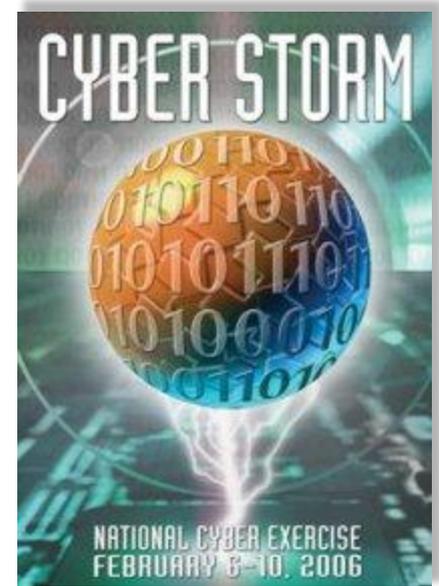


**Homeland  
Security**

# Cyber Exercises

- CyberStorm Series
  - Congressionally required Tier II exercise
- Cyberstorm III
  - September 30 – October 1, 2010
  - First test of the National Cybersecurity and Communications Integration Center (NCCIC)
- After actions and lessons-learned TBD (LLIS.gov)

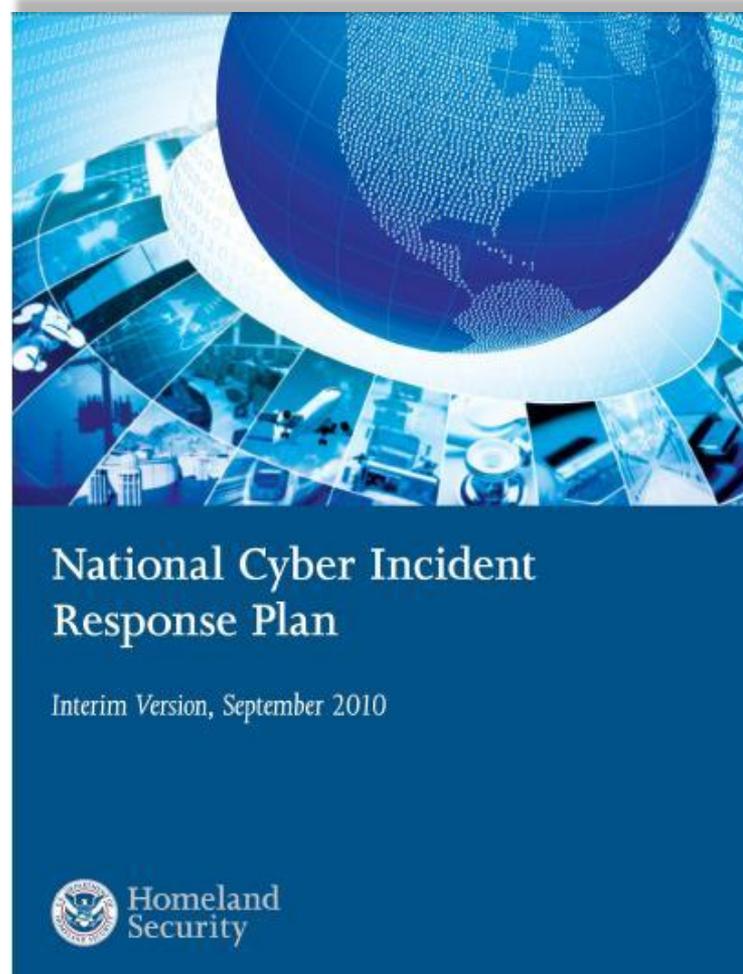
**“In Cyber Storm I, we attacked the Internet, in Cyber Storm II, we use the Internet as the weapon, in Cyber Storm III, we're using the Internet to attack itself.” – Brett Lambo, Exercise Program Director**



**Homeland  
Security**

# National Cyber Incident Response - 1

- National Cyber Incident Response Plan (NCIRP), Interim Version (September 2010)
- The NCIRP supplements the Cyber Incident Annex to the National Response Framework (NRF) and ultimately is a companion document to the NRF.



**Homeland  
Security**

# National Incident Response - 2

- National Cyber Risk Alert Levels (NCRAL)
  - NCIRP (Interim) designates the National Cyber Risk Alert Level (NCRAL) as the means of determining and promulgating the cyber risk to the Nation.
  - Final NCRAL to-be released in 2011 and include alert level definitions, guidance on triggers for each level, and tailored readiness options (TRO).

Label	Description of Risk	Level of Response
<b>Severe</b>	Highly disruptive levels of consequences are occurring or imminent	Response functions are overwhelmed, and top-level national executive authorities and engagements are essential. Exercise of mutual aid agreements and Federal/non-Federal assistance is essential.
<b>Substantial</b>	Observed or imminent degradation of critical functions with a moderate to significant level of consequences, possibly coupled with indicators of higher levels of consequences impending	Surged posture becomes indefinitely necessary, rather than only temporarily. The DHS Secretary is engaged, and appropriate designation of authorities and activation of Federal capabilities such as the Cyber UCG take place. Other similar non-Federal incident response mechanisms are engaged.
<b>Elevated</b>	Early indications of, or the potential for but no indicators of, moderate to severe levels of consequences	Upward shift in precautionary measures occurs. Responding entities are capable of managing incidents/events within the parameters of normal, or slightly enhanced, operational posture.
<b>Guarded</b>	Baseline of risk acceptance	Baseline operations, regular information sharing, exercise of processes and procedures, reporting, and mitigation strategy continue without undue disruption or resource allocation.



# Cyber Security Evaluation Program

“In partnership with public and private sectors, improve cyber security across all critical infrastructure sectors”

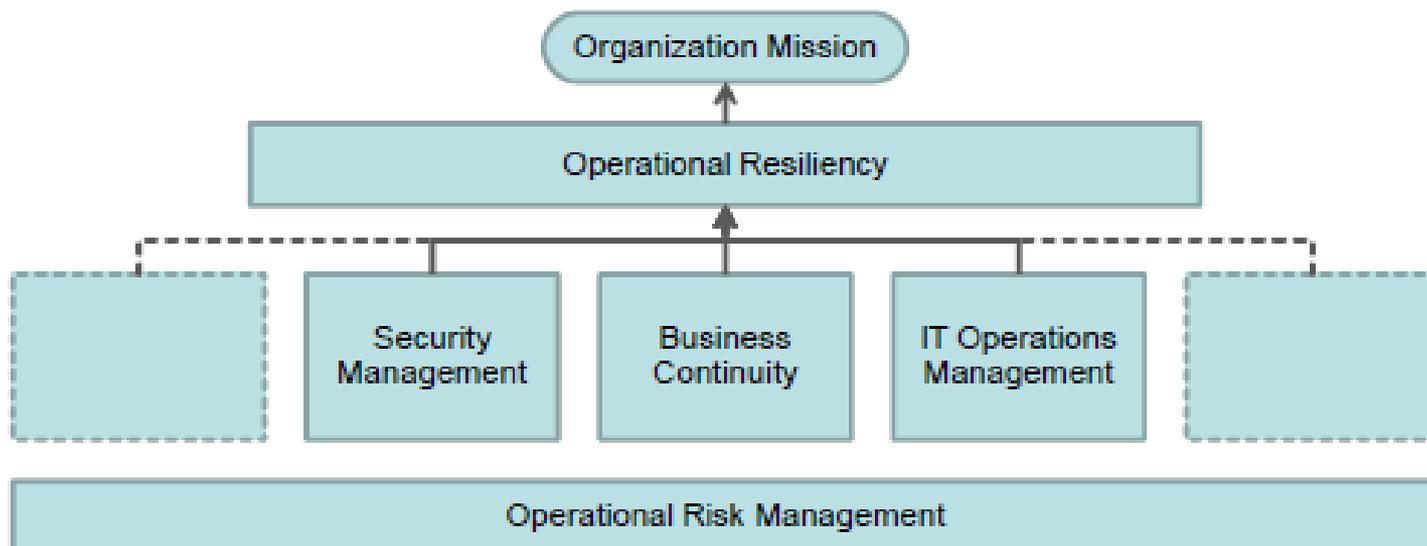
- Conducts voluntary cyber security assessments across all 18 CIKR Sectors, within state governments, and for large urban areas.
- Employs a portfolio of assessment tools, techniques, and analytics, ranging from those that can be self-applied to those that require expert facilitation or mentoring outreach.
- Seeks to measure key performances in cyber security management.
- For more information, visit [www.dhs.gov/xabout/structure/editorial\\_0839.shtm](http://www.dhs.gov/xabout/structure/editorial_0839.shtm) or contact the program at [CSE@dhs.gov](mailto:CSE@dhs.gov).



**Homeland  
Security**

# Resilience-based Reviews

A capability-based (versus a control-based) review of the level of operational resilience of an organization



- Operational resilience affects the ability to meet the organization's mission
- Convergence of IT operations, security, and business continuity affects the level of operational resilience



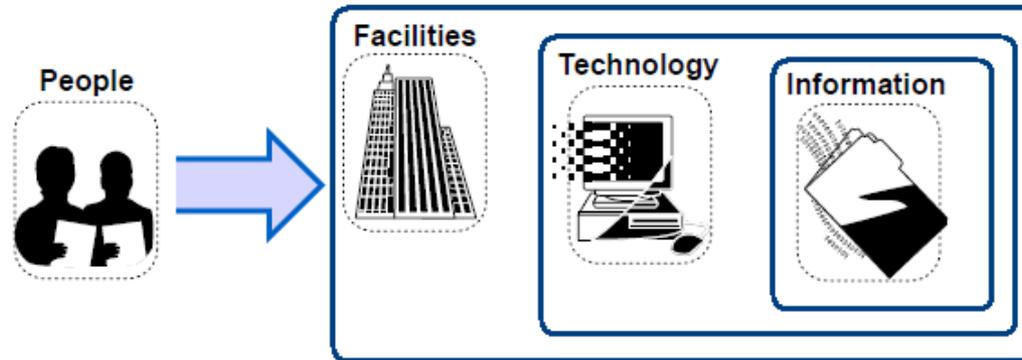
# Service-oriented Approach

- One of the foundational principles of the CRR is the idea that an organization deploys its assets to support specific missions
- A service-oriented approach also helps to narrow and focus the discussion and question scope during the CRR
- The CRR takes an identified critical service as representative of the organization's services as a whole
  - **Critical services** are those that are so critical to the success of the organization that, if disrupted, would severely impact continued operations or success in meeting the organization's missions

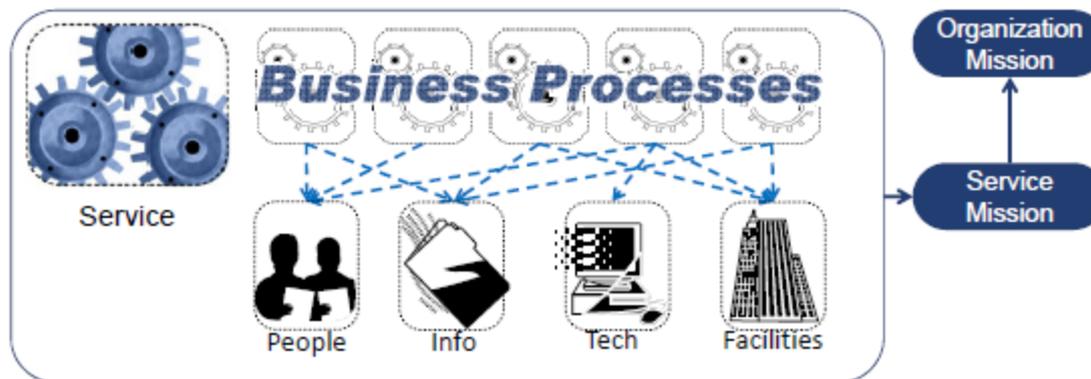


# Cyber Assets

- The CRR focuses on 4 key classes of interrelated cyber assets:

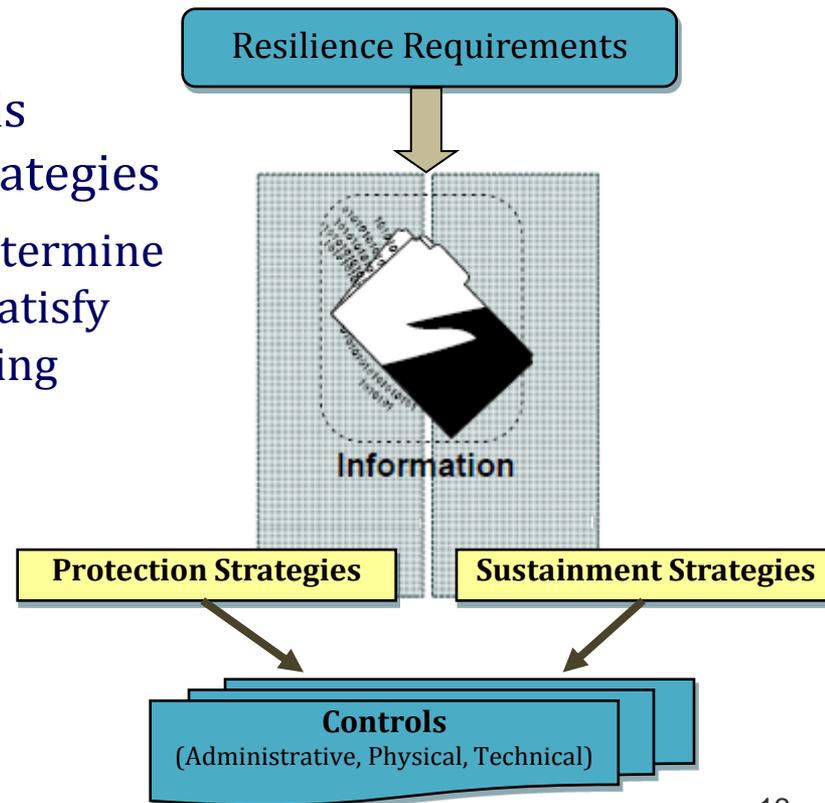


- Failure in any of these assets may result in a cascading impact on related business processes, services, and the organization's mission



# Resilience of Assets

- To ensure **operational resilience** at the **service** level, assets related to the delivery of the service must be afforded:
  - **Protection:** manage *conditions* of risk (i.e., protect from threats)
  - **Sustainment:** manage *consequences* of risk (i.e., sustain under adverse conditions)
- **Resilience requirements** form the basis for asset protection and sustainment strategies
  - Protection and sustainment strategies determine the type and level of controls needed to satisfy resilience requirements (and thus, ensuring operational resilience)



# Resilience Domains

- 10 key categories:
  1. Asset Management
  2. Configuration and Change Management
  3. Training & Awareness
  4. Vulnerability Management
  5. Incident Management
  6. Service Continuity
  7. Environmental Control
  8. External Dependency Management
  9. Situational Awareness
  10. Risk Management

Each category is an area of discovery into the current state of cyber security management practices instantiated by:

- Strategies, standards, policies, plans, processes, procedures in place
- Communication with and notification to all those who need to know
- Execution and analysis in a consistent, repeatable manner
- Alignment of practices in one domain with those in the other categories



# Benefits of Cyber Resilience (Focus)

- Allows the organization assessed to frame asset protection against the core/key services being delivered (i.e., critical infrastructure services)
- Allows the organization to reflect upon the security of key components and assets that must be available to deliver the service, in terms of:
  - People's actions, responsibilities, and roles e.g., security practitioners)
  - Systems, networks, and information (technologies)
  - Internal processes and procedures implementing decision-making and security management
  - Key facilities (instrumental in delivering the service)



# 1. Asset Management Objectives

- **Consistently identify assets in a common repository, include:**
  - Asset description, such as physical location, business owners, technical administrators, sensitivity, criticality, etc.
  - Assets provided or maintained by external parties
  - How and from where assets are accessed
- **Asset-to-service traceability**
  - Identify assets required to deliver each service
  - Trace business managers to the assets that support their services
- **Identify asset protection (i.e., security) and sustainment (i.e., continuity) requirements** based on the needs of the critical service
- **Uniformly review and manage the impact of changes to assets**
  - Ensure that changes do not introduce additional exposure to risk
  - Ensure that asset description and protection and sustainment strategies are updated as appropriate



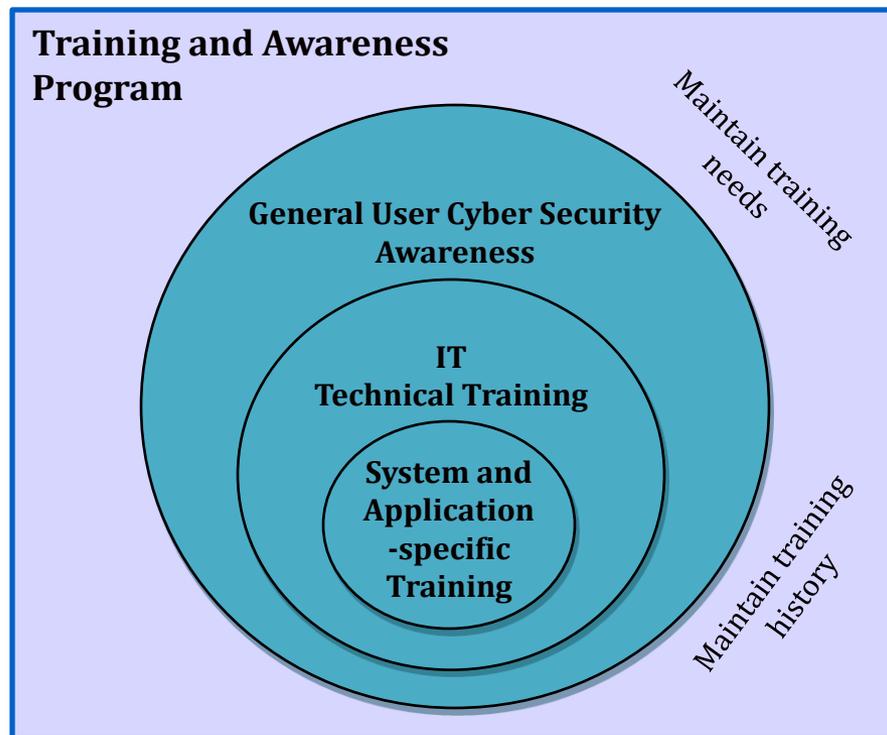
## 2. IT Management Objectives

- **Develop effective protection and sustainment strategies** to support confidentiality, integrity, and availability of information and technology assets
  - Determine standards for applying security controls
  - Set baseline configurations
  - Provide guidance on appropriate labeling and handling of information
- **Identify criteria for changing protection strategies for IT assets**
  - Consider what causes change in configuration of security controls
- **Identify and mitigate operational risk**
  - Consider risk assessments and business impact analysis in selecting and changing security controls
- **Validate the function of security controls**
  - Consider independent audits and continuous monitoring of security controls



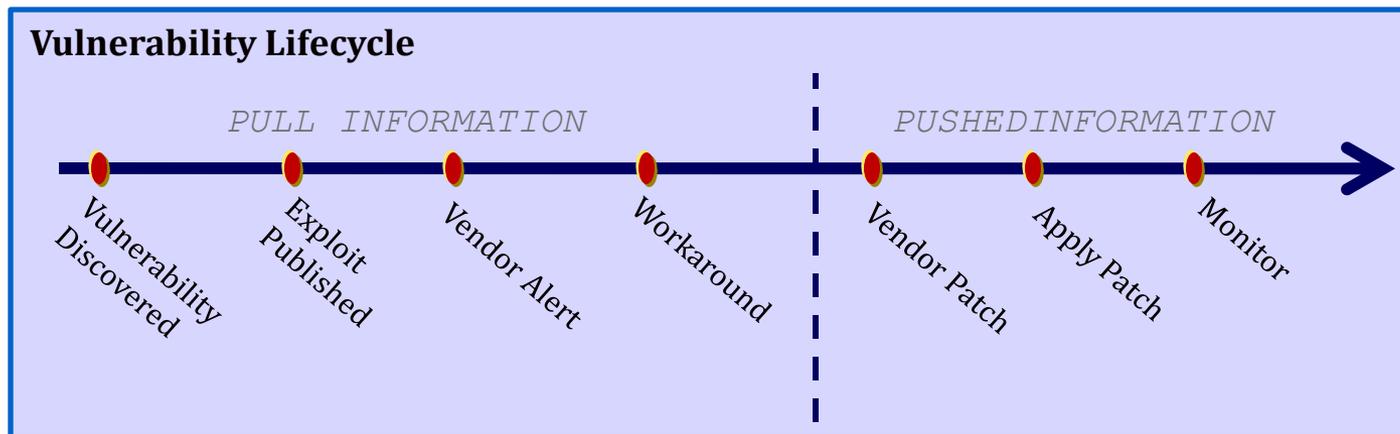
## 2. IT Management Objectives *(cont.)*

- Ensure effective cyber security training and awareness



# 3. Vulnerability Management Objectives

- Establish a repeatable and effective vulnerability management process
- Define criteria for consistent evaluation of vulnerabilities, and align criteria with the role a given asset plays in the production of service



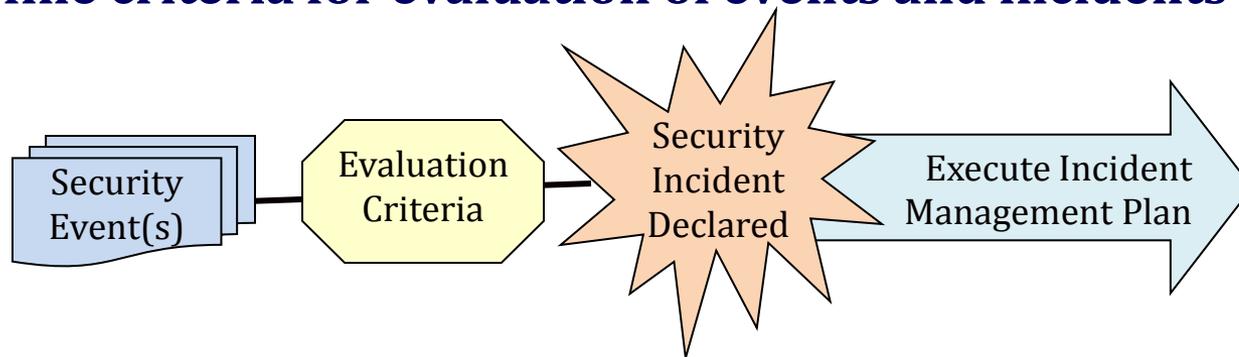
# 4. Incident Management Objectives

- Establish a repeatable and effective incident management process



- Includes internal/external notification, communication, reporting, documentation, and tracking throughout the incident management process

- Define criteria for evaluation of events and incidents



# 5. Service Continuity Objectives

- **Identify and document critical services** to ensure continuity of essential operations in case of a disruption, and consider:
  - Critical suppliers and customers
  - Upstream and downstream mitigation plans, with RTOs/RPOs
- Identify and document the process and criteria to **evaluate and prioritize critical services**
- **Define service resilience requirements** for identified critical services
- **Develop service continuity plans**, which may include plans for:
  - Continuity of government
  - Business continuity
  - Disaster recovery
- **Test and exercise plans** with enough frequency to be actionable
  - Update plans as a result of tests and exercises



# 6. Environmental Control Objectives

- **Consistently identify and document facilities (and sub-facilities)** that house IT assets critical to the delivery of services
  - Refer to asset inventory to ensure that physical safeguards align with the resilience requirements
- **Prioritize facilities** relative to their importance in the delivery of services
- **Consistently identify and assess physical risk and align it to the delivery of services**
  - Periodically review the effectiveness of the facility security controls that contribute to securing and sustaining IT assets
  - Consider geographic issues when making decisions regarding facility selection and protection
- **Periodically review and validate physical security strategies** by employing independent audits of facility security controls
  - Use audits results to make changes to facilities
  - Document controls applied to facilities



# 7. External Dependency Management Objectives

- **Identify dependencies on external parties, products, and services**
  - Analyze and prioritize dependencies by criticality
- **Identify and reduce exposure to risk from dependent relationships**
  - Develop mitigation plans for failure of external parties, products, or services
  - Require external parties to provide evidence of meeting resilience requirements
  - Actively monitor performance of providers against requirements
  - Implement corrective actions
- **Establish and review cyber security agreements with third parties**
  - Include clauses related to cyber security management in agreements
  - Regularly review agreements to ensure that requirements are met
- **Recognize and mitigate dependency on public services**
  - Identify and set performance expectations in event of an incident
  - Integrate public service providers into continuity exercises
  - Define communication/notification plans, and identify contacts



# 8. Situational Awareness Objectives

- **Active discovery of relevant, current cyber security information**
  - Identify common sources for threats, vulnerabilities, current events
  - Identify forums focusing on resilience, security, or emergency preparedness
- **Consistently evaluate sources of information for trustworthiness**
  - Including analysis of incidents to deepen understanding of reliable sources
- **Define formal levels of readiness**
  - Identify pre-determined behaviors and activities aligned with each level of readiness
- Analyze and communicate current events to ensure that all areas of operation **perform under a common operating picture**
- **Predict threats and events** to enable a more defensive posture for its operations



# Evaluation Lessons-Learned - 1

- Things You ALREADY Know
  - High amount of institutional and longitudinal knowledge in employees (most with 10+ years of experience with DPWs)
  - High dependence on “self” and “limited” IT staff (from within formal IT Departments)
  - Low amount of documentation on what has happened to the system since it was originally purchased/installed (i.e., security configurations, patches / vulnerabilities, etc)
- Things You May be SURPRISED About
  - Incidents are governed by a “plan” but it accounts for only a limited space of threats (e.g. viruses and “faults”)
  - Continuity planning exists as mostly Disaster Recovery Plans but not continuity of operations plans
  - Limited external dependencies (beyond IT staff)



# Evaluation Lessons-Learned - 2

- Observations: From CIKR Sites and State and Local Governments
  - Participants generally do not align assets to their organizational mission.
  - Participants are often challenged to understand if their protection and sustainment strategies are effective.
  - Participants are often challenged to harmonize physical and logical security management activities.
  - Participants are often aware of external dependent relationships , however, the management of those external dependencies is often not aligned to the organizational mission.
  - Participants often do not define vulnerability evaluation criteria and therefore tend to be uneven in determining remediation actions.
  - Participants have experienced denial of service attacks as a result of malware (spam/social engineering) and system failures (caused by physical and technical means).





# Homeland Security

## Contact Information

Bradford Willke ([bradford.willke@dhs.gov](mailto:bradford.willke@dhs.gov))

Mid-Atlantic Cyber Security Advisor

Cyber Security Evaluation Program

National Cyber Security Division

Office of Cyber Security and Communications

Program Email: [CSE@hq.dhs.gov](mailto:CSE@hq.dhs.gov)



Homeland  
Security