Moving Toward Cyber Resilience

Bradford Willke, Cyber Security Advisor (Mid-Atlantic Region)

Cyber Security Evaluation Program
National Cyber Security Division

Central Ohio Infragard
Columbus, Ohio
27 July 2011

History

- National Cyber Security Division (NCSD) created in June 2003 to serve as the national focal point for cybersecurity and to coordinate implementation of the *National Strategy to Secure Cyberspace* (the "Strategy") issued in February 2003.
- Part of the National Protection and Programs Directorate (NPPD), whose mission is to advance the Department's risk-reduction mission.
  - Reducing risk requires an integrated approach that encompasses both physical and virtual threats and their associated human elements.
- In 2006, Congress created the Office of Cybersecurity and Telecommunications within NPPD.
- The office has been renamed the Office of Cybersecurity and Communications (CS&C) and is led by an Assistant Secretary.
- NCSD is a division within CS&C.

Vision and Mission

The **National Cyber Security Division (NCSD)** serves as the Federal Government's lead in assessing, mitigating and responding to cyber risks in collaboration with Federal, State and local governments, the private sector, academia, and international partners.

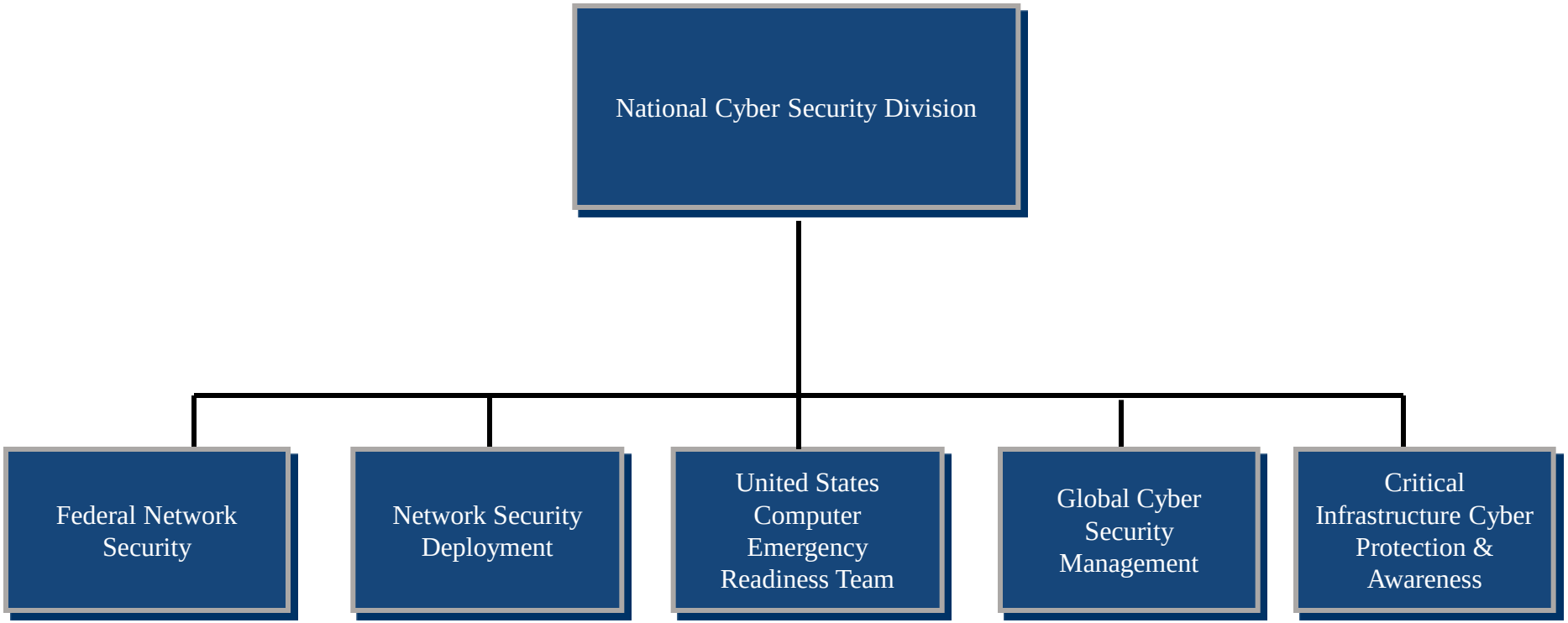
Mission

To work collaboratively with Federal, State and local governments, private sector, and international partners to protect and secure cyberspace and America's critical information infrastructure.

Goals

- Manage cyber risk to the Nation;
- Improve national cyber protection, response, and recovery capabilities;
- Empower and collaborate with all security partners to secure cyberspace and cyber assets; and
- Build and maintain a highly respected and globally recognized organization to advance the Nation's cybersecurity.

NCSD Branches



Initiatives in Critical Cyber Infrastructure Protection (Ongoing and Updates)

- Regional Cyber Security Advisors
- Outreach and Awareness
- Industrial Control System – Computer Emergency Readiness Team (ICS-CERT)
- Cyber Exercises and National Cyber Incident Response
- Cyber Security Evaluations

CIA

"Web sites are the low-hanging fruit." - Richard Stiennon

- **Background**
  - The CIA's Web site was taken down for a couple of hours, by LulzSec as part of a string of embarrassing Web site disruptions the group had pulled off. The assault on the CIA was by denial of service, or overloading the site's server with requests for access.

- **Stolen Data**
  - LulzSec apparently hacked the CIA more to poke fun and highlight vulnerabilities than to cause real damage, but the fact that the group could penetrate Web sites and harvest system administrators' credentials underscores the risks of failing to secure sites.

Source: "CIA Web site hacked; group LulzSec takes credit," June 15, 2011, The Washington Post
http://www.washingtonpost.com/national/national-security/cia-web-site-hacked/2011/06/15/AGGNphWH_story.html

CIA

- **How The Attacks worked**
  - "Web sites are running on a server. Once you completely own the server that the Web site is on, you can watch the insiders log in and record their activity, and that can be a front door into the organization." - Richard Stiennon, a cyber-expert and author of "Surviving Cyberwar."

- **Possible Motive**
  - LulzSec's motivation appeared to be for grins and giggles. "This is a very old hacker mentality, which is if you're vulnerable, you're stupid and deserve to be embarrassed and taken out." - Richard Stiennon. LulzSec has an "anarchistic" agenda and is against government control of information, much as they're against media control of music and movies."

Cyber Security Advisor Program

- Strategic Goals
  - Provide personnel to assist in the identification, assessment, and protection of CI/KR locally and regionally, throughout the U.S.
  - Support cyber security risk management efforts at the State and Local level with regard to homeland security initiatives.
- Operation Goals
  - Act as on-site cyber security specialists to provide a Federal resource to regions, communities, and businesses.
  - CSA regions cover 10 designated geographic areas; aligned to the FEMA regions.

Cyber Security Advisor – Mission Objectives - 1

- Lead and support cyber risk analyses of regional and local CI/KR.
- Assist in the review and analysis of cyber security of regional and local CI/KR.
- Provide guidance on evaluating established cyber security practices and capabilities.
- Provide regional and local stakeholders (in Critical Infrastructure and Key Resource sectors as well as state and local government) with access to updated Department of Homeland Security capabilities, including:
  - New tools, technologies, and methods.
  - Recommended practices for protection and mitigation strategies.

Cyber Security Advisor – Mission Objectives - 2

- Keep communities informed of national cyber security policy context and initiatives.
- Convey local concerns and sensitivities to the National Cyber Security Division.
- Relay disconnects between local, regional, and national protection activities.
- Communicate requests for Federal training and exercises.
- Provide support to officials responsible for (national special) security events planning.

Cyber Security 'Fusion' – Nothing but Questions

- How do we facilitate information sharing on site-specific cyber security capabilities and dependencies, answering:
  - How a site manages cyber security (threat, vulnerability, and consequence)
  - How third-parties provide operational support
  - How IT and Communications Sectors' (may) create external dependencies
  - How people, procedures, technology, and facilities (may) create internal dependencies
- How do we facilitate information sharing on multi-site, regional cyber security, answering:
  - How sites learn and share information about cyber security

    i.e., via ISACs, InfraGard chapters, Business Coalitions, SCCs, EOCs, Fusion Centers, Security Vendors, etc.
  - How sites prepare for or will respond to incidents and contingencies

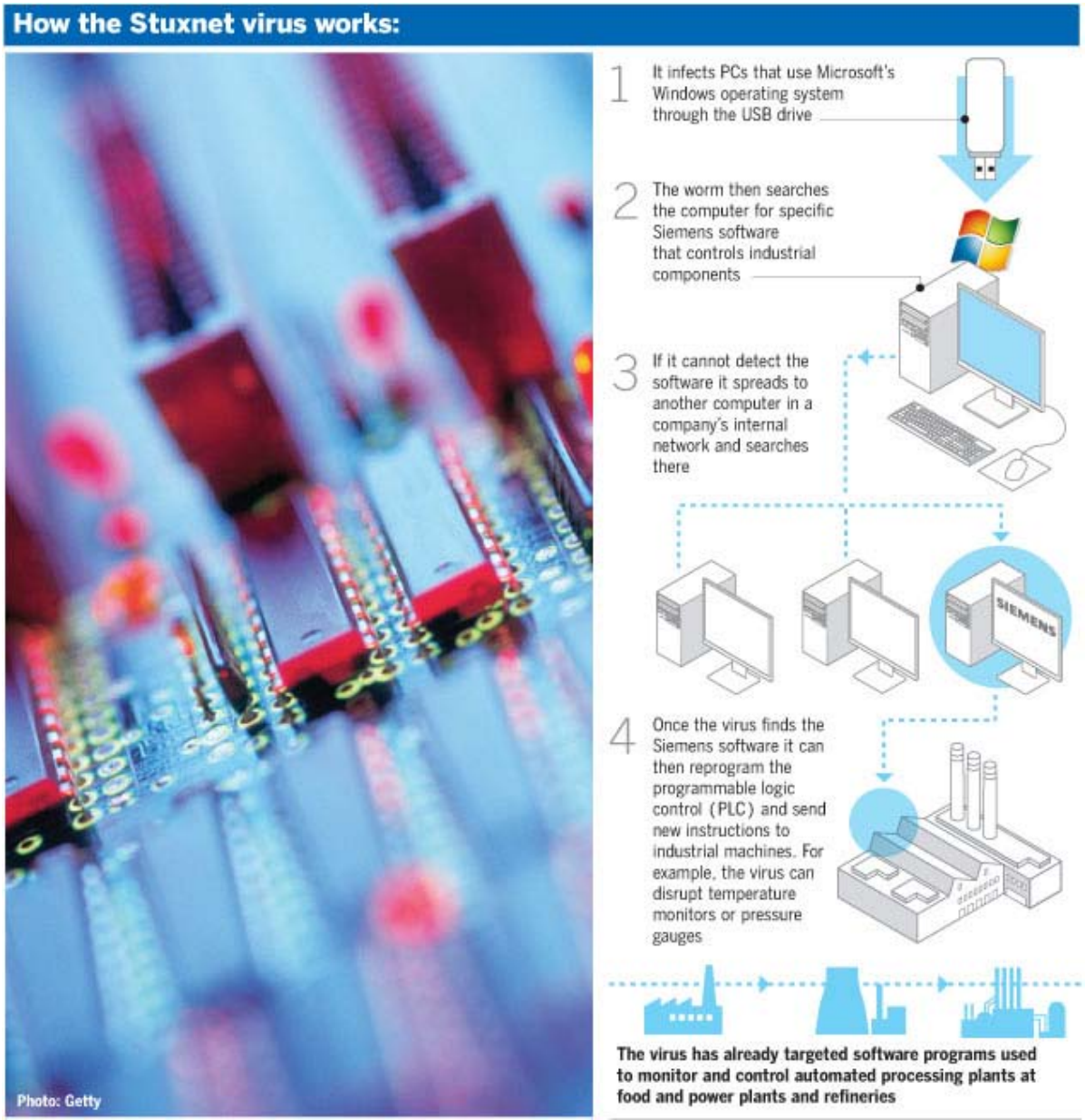
Outreach and Awareness

- 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

Stuxnet

"We have not seen this coordinated effort of information technology vulnerabilities, industrial control exploitations, completely wrapped up in one unique package. For us, to use a very overused term, it's a game changer. Stuxnet … modifies the physical settings of a process control environment."
-- Seán P. McGurk



Source: MALWARE CALLED STUXNET ATTACKS 45,000+ COMPUTERS, Bewreck.com (last visited Dec. 7, 2010)

Stuxnet

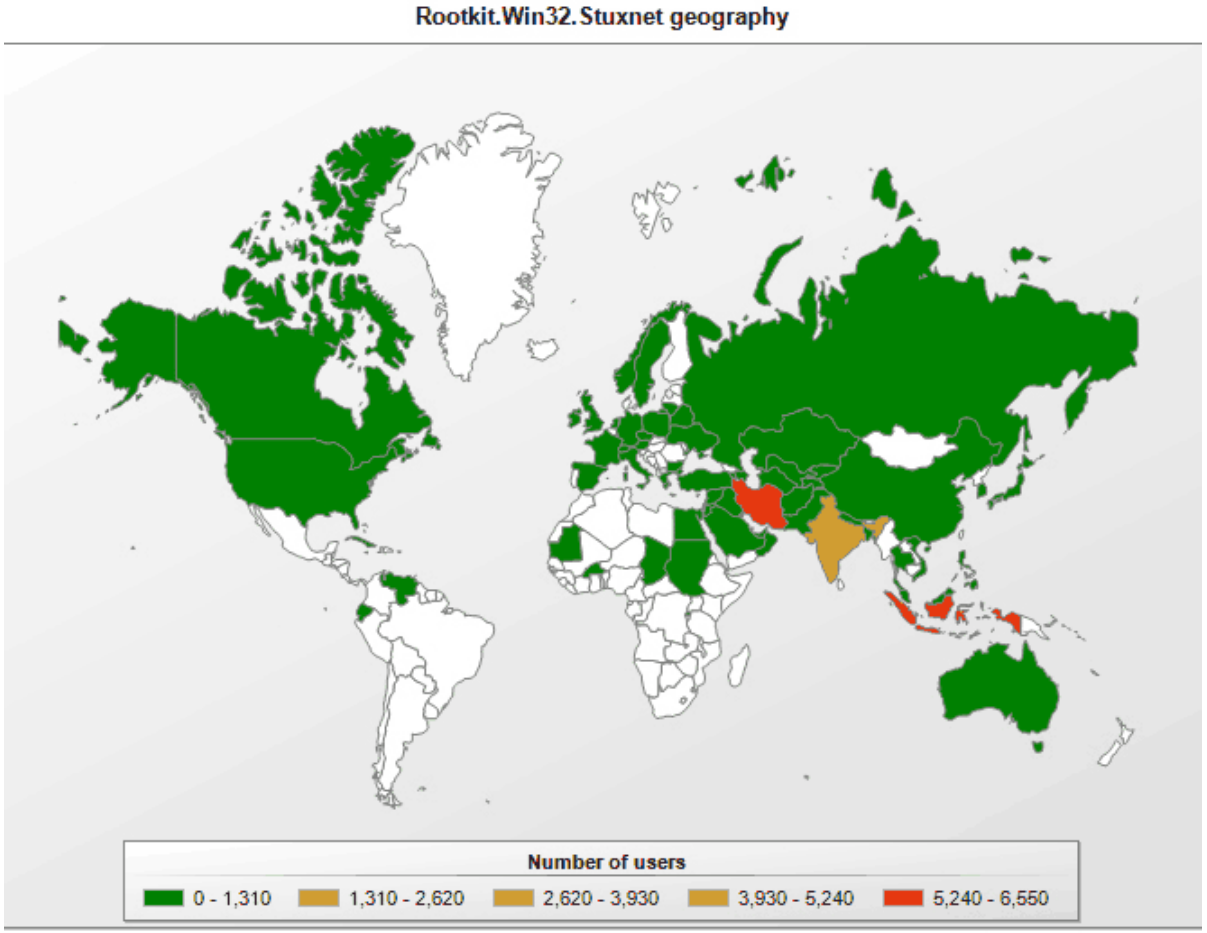
"The world's first precision cybermunition" - Hunting an Industrial-Strength Computer Virus Around the Globe, PBS Newshour, Oct. 1, 2010.

Possible developers

- United States
- Israel
- United Kingdom
- Russia
- China
- France

Countries affected

- Iran
- Indonesia
- India
- Pakistan
- Germany
- China
- United States



Stuxnet

"Proliferation [of cyber weapons] is a real problem… We have about 90 days to fix this [new vulnerability] before some hacker begins using it." – Melissa Hathaway

- **Suspected target**
  - Iran's SCADA controlled nuclear facilities
- **Motive**
  - Not designed to steal information, but rather designed to disrupt control systems and disable operations
- **Effects**
  - Reports vary from several centrifuges shutting down for days in November, to several centrifuges blowing up
- **Possible consequences**
  - National Security concerns
  - A cyber arms race
  - Falling into "the wrong hands" and becoming more potent
  - Unknown and/or unintended secondary or tertiary effects

Source: PAUL K. KERR ET AL., THE STUXNET COMPUTER WORM: HARBINGER OF AN EMERGING WARFARE CAPABILITY (Congressional Research Service, Dec. 9, 2010).

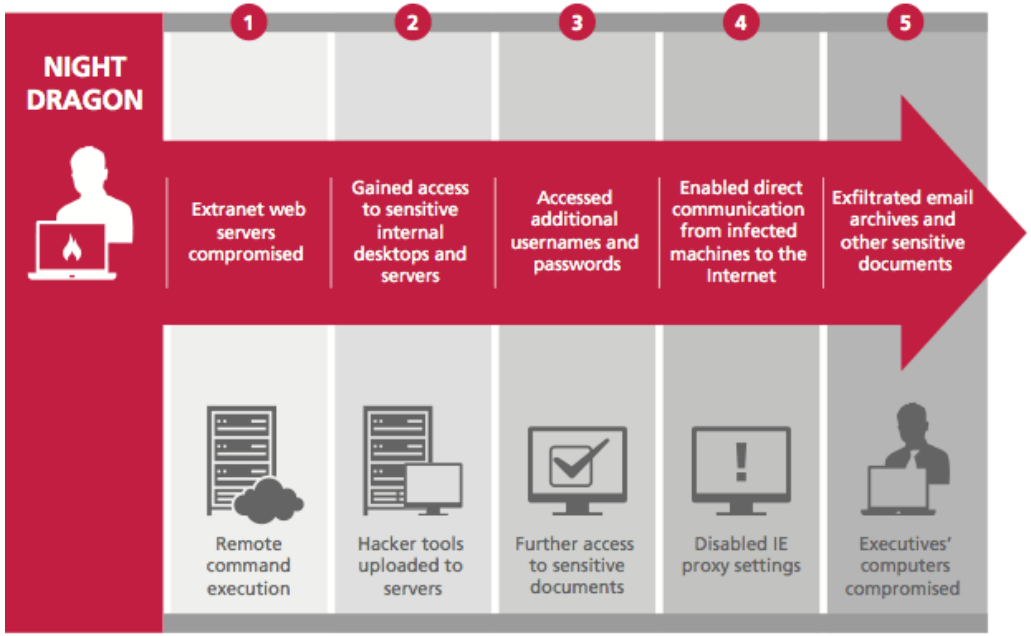
Night Dragon

- **Background**
  - Over the course of the last two to four years, attackers penetrated the networks of several multinational oil and other energy companies, stealing sensitive information, according to a report by McAfee.
- **Stolen Data**
  - Stolen files included financial documents, information on oil and gas field production systems, as well as data from supervisory control and data acquisition (SCADA) systems controlling industrial processes.
- **Possible Source**
  - McAfee believes the attacks are from China, carried out by a coordinated effort, as opposed to attacks launched by freelance or unprofessional hackers.
- **Espionage**
  - McAfee believes that the attacks were designed to steal information, not to sabotage any equipment.

Night Dragon

- **How the Attacks Worked**
  - The attackers penetrated company networks by compromising Web servers and desktops.
  - Attackers misused administrative credentials and used remote administration tools to steal data.

- **Possible Implications**
  - Attacks are being carried out by well-coordinated groups.
  - Attacks have moved beyond government targets and on to commercial ones.
  - Night Dragon techniques can be effective on any industry, not just the energy sector.
  - Attacks have begun to target specific intellectual property; protection of such data is becoming more important.



Sources: "Data Theft Attacks Besiege Oil Industry, McAfee says," Cnet.com, February 10, 2011; "Global Energy Cyberattacks: 'Night Dragon,'" McAfee, February 10, 2011

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/

Booz Allen Hamilton

- **Background**
  - A group of hackers claimed to have penetrated a computer server of Booz Allen Hamilton and released a list of more than 90,000 military email addresses and encrypted passwords and deleted 4 GB of source code, calling the hack "Military Meltdown Monday".
- **Stolen Data**
  - In addition to the military email addresses, passwords, and deleted source code, the hacker group also said that it has uncovered "all sorts of other shady practices" by Booz Allen, including potentially illegal surveillance systems, corruption between company and government officials and warrantless wiretapping.

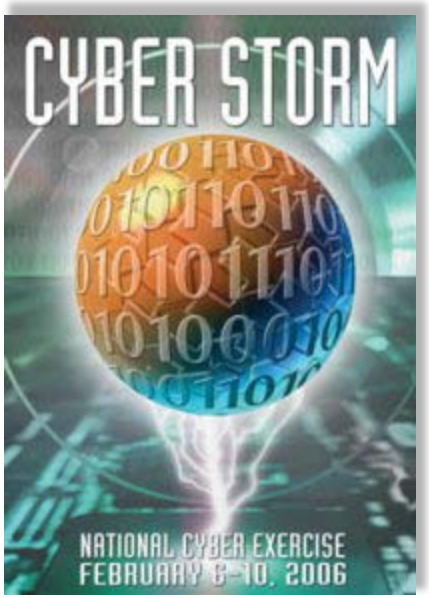
Sources:
"Booz Allen Hamilton Hack Reveals Military Email Addresses," July 11, 2011, HUFFPOST TECH
http://www.huffingtonpost.com/2011/07/11/booz-allen-hamilton-hack_n_895147.html

Booz Allen Hamilton

- **Possible Source**
  - The hacker group works under the label "AntiSec," which is believed to consist of the hacker groups Anonymous and LulzSec. The data breach came three days after the group claimed responsibility for breaking into the system of IRC Federal, a contractor for the Federal Bureau of Investigation.

- **How the Attacks Work:**
  - The hackers said it was easy to break into the firm's own network, which "basically had no security measures in place."
  - Hackers can use such emails to access government computer systems by engaging in targeted attacks called "spear phishing," or appearing to be a trusted sender and tricking recipients into opening malware.
  - Many of these successful hacks of government systems have occurred through people being directly phished.
  - Hackers can "get a foothold on a computer and put a virus on it and that virus can collect all the passwords or documents they access. It could open people up to more exposure to these types of attacks and make it easier for the system to be compromised.

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

Lockheed Martin

- **Background**
  - A major online attack was launched against the networks of Lockheed Martin, the country's largest defense contractor. Hackers reportedly exploited Lockheed's VPN access system, which allows employees to log in remotely by using their RSA SecurID hardware tokens.

- **Stolen Data**
  - Lockheed Martin described the attack as "significant and tenacious." But it said its information security team "detected the attack almost immediately and took aggressive actions to protect all systems and data." As a result, the company said, "our systems remain secure; no customer, program, or employee personal data has been compromised."

Sources:
"Lockheed Martin Suffers Massive Cyberattack," May 31, 2011, Information Week
http://www.informationweek.com/news/government/security/229700151

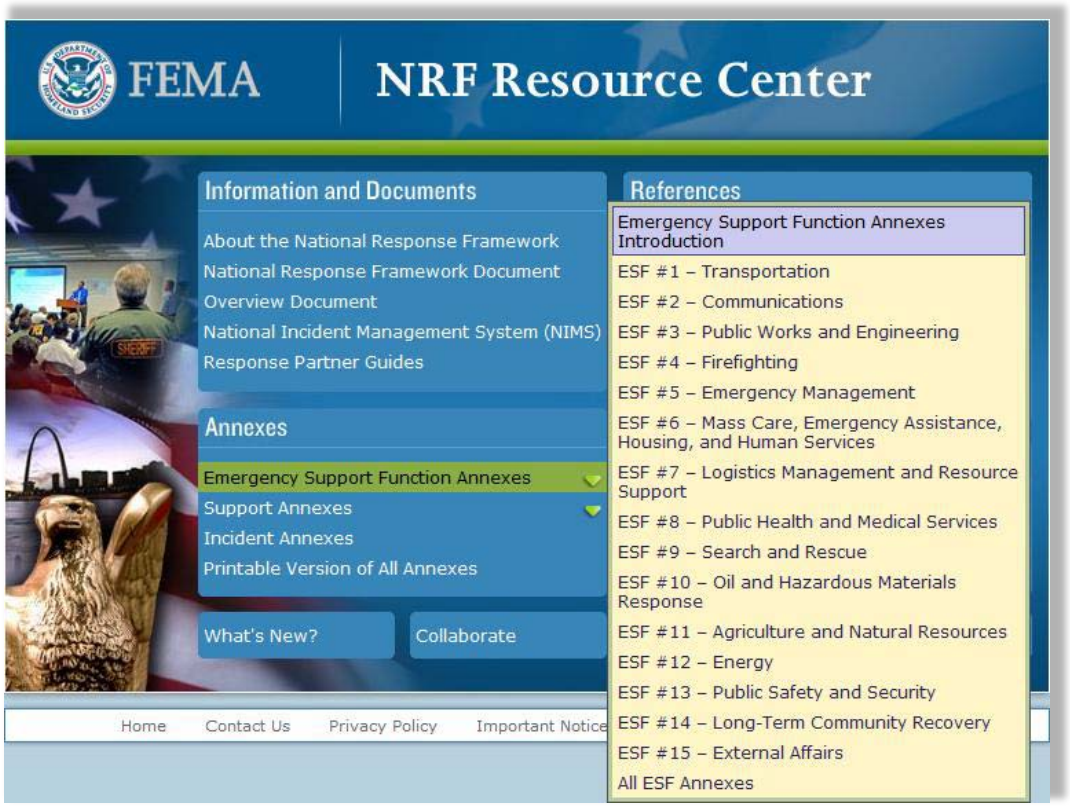
Lockheed Martin

- **Possible Source**
  - There was a breach in EMC's RSA division, which manufactures SecurID. "Since then, there have been malware and phishing campaigns…seeking specific data linking RSA tokens to the end user, leading us to believe that this attack was carried out by the original RSA attackers," Rick Moy, president and CEO of NSS Labs.
  - Attackers apparently possessed the seeds--factory-encoded random keys--used by at least some of Lockheed's SecurID hardware fobs, as well as serial numbers and the underlying algorithm used to secure the devices.
  - From there, attackers reportedly gained access to the company's internal network.

- **Outcome**
  - This was very subtle breach and not easy to spot.
  - Lockheed Martin's swift detection of the attack helped avert potential disaster.
  - That same day that Lockheed Martin detected the attack, all remote access for employees was disabled.
  - The company told all telecommuters to work from company offices for at least a week.
  - Then the company informed all remote workers that they'd receive new RSA SecurID tokens.
  - Lockheed Martin told all 133,000 employees to reset their network passwords.

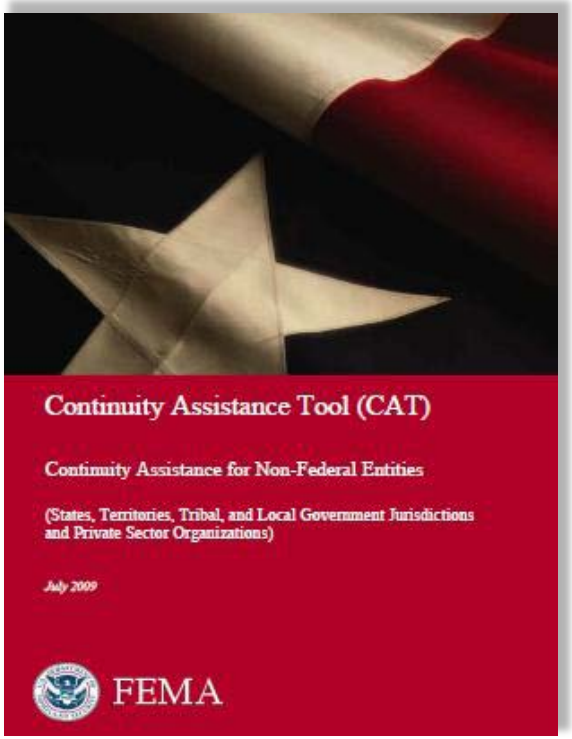
National Incident Response - 1

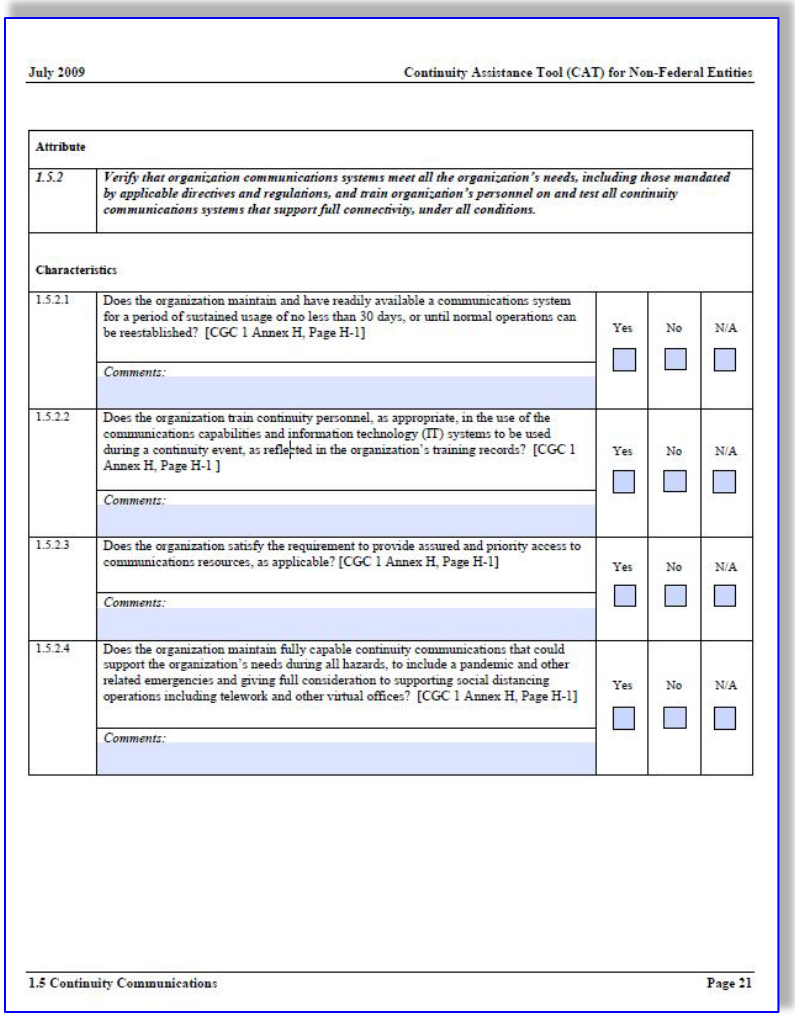
- The NCIRP cites specific authorities (administrative rules and legislation), outlines key roles and responsibilities of national, state and local level, private industry, NGOs, etc.
  - Cites to the Emergency Support Functions (ESF), specifically to ESF#2 for Communications and ESF #15 for External Affairs.



National Incident Response - 2

- Relationship to Federal Continuity Directive – 1 (FCD-1) and the non-Federal *Continuity Guidance Circular* (CGC-1)





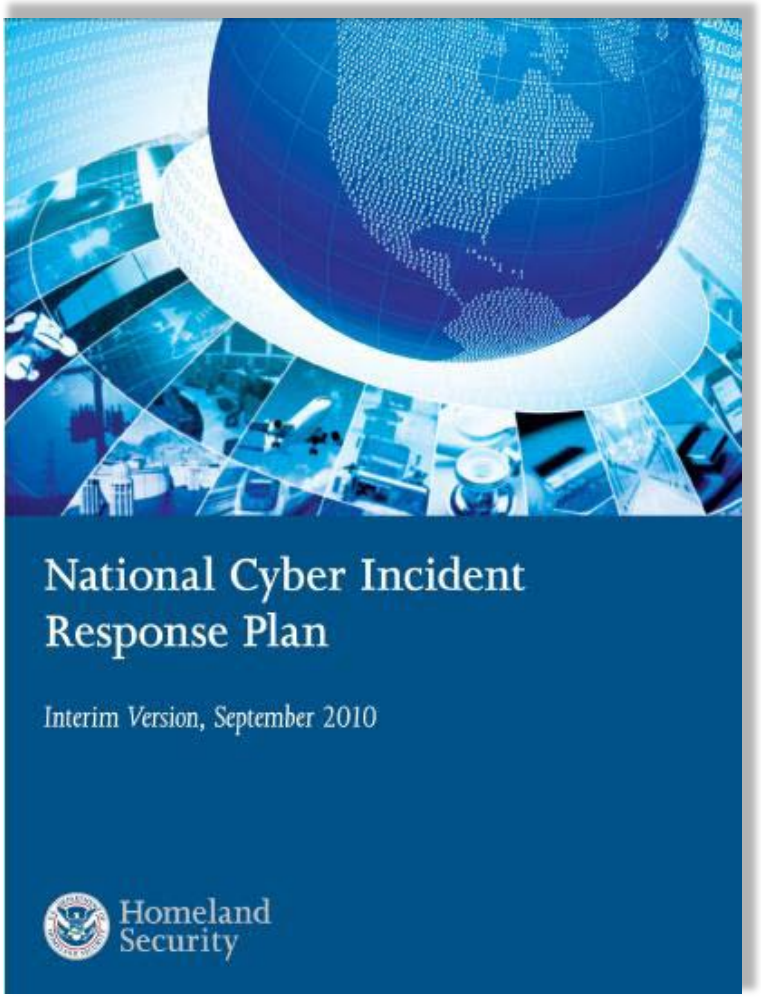
July 2009 — Continuity Assistance Tool (CAT) for Non-Federal Entities

Attribute				
1.5.2	***Verify that organization communications systems meet all the organization's needs, including those mandated by applicable directives and regulations, and train organization's personnel on and test all continuity communications systems that support full connectivity, under all conditions.***			
Characteristics				
1.5.2.1	Does the organization maintain and have readily available a communications system for a period of sustained usage of no less than 30 days, or until normal operations can be reestablished? [CGC 1 Annex H, Page H-1] *Comments:*	Yes ☐	No ☐	N/A ☐
1.5.2.2	Does the organization train continuity personnel, as appropriate, in the use of the communications capabilities and information technology (IT) systems to be used during a continuity event, as reflected in the organization's training records? [CGC 1 Annex H, Page H-1] *Comments:*	Yes ☐	No ☐	N/A ☐
1.5.2.3	Does the organization satisfy the requirement to provide assured and priority access to communications resources, as applicable? [CGC 1 Annex H, Page H-1] *Comments:*	Yes ☐	No ☐	N/A ☐
1.5.2.4	Does the organization maintain fully capable continuity communications that could support the organization's needs during all hazards, to include a pandemic and other related emergencies and giving full consideration to supporting social distancing operations including telework and other virtual offices? [CGC 1 Annex H, Page H-1] *Comments:*	Yes ☐	No ☐	N/A ☐

1.5 Continuity Communications — Page 21

National Cyber Incident Response - 1

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



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
Severe	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.
Substantial	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.
Elevated	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.
Guarded	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 Advisors: Integration with NCIRP / NCRAL System

Guarded

- **Role:** CSA **performs normal duties**, which includes general outreach, awareness, and evaluation activities with CIKR providers to improve cyber preparedness , risk mitigation, and incident response
- **Externally:** CSA answers questions regarding advisory level status

Elevated

- **Role:** In addition to normal duties, CSA **increases liaison with critical infrastructure groups**
- **Externally:** CSA helps to notify *affected communities of interest* and answers questions regarding advisory level change (and status)
- **Internally:** CSA coordinates with NCCIC Assess and Assist Branch, to include awareness of situational reports, with an emphasis on general preparedness and readiness

Substantial

- **Role:** In addition to normal duties, CSA **increases liaison** with critical infrastructure groups, and specifically **with likely (direct and indirect) targets of attack** based on intelligence
- **Externally:** CSA helps to notify *affected communities of interest* and *specific/likely targets,* and answers questions regarding advisory level change (and status)
- **Internally:** CSA coordinates with NCCIC Assess and Assist and Liaison Branches, to include participation in daily communications, with an emphasis on specific preparedness and readiness

Severe

- **Role:** CSA **suspends normal duties to work directly with affected party** (or parties), but continues to notify *related communities of interest* and to answer questions regarding advisory level change (and status)
- **Externally:** CSA works directly with affected party of attack (i.e., on-site or at coordinating location), performing damage assessments, incident coordination, and root-cause analyses.
- **Internally:** CSA coordinates with NCCIC Assess and Assist and Liaison Branches, and US-CERT and/or ICS-CERT (depending on scenario), with an emphasis on incident coordination and management

Sony

- **Background**
  - Credit card data of PlayStation users around the world may have been stolen in a hack that forced Sony Corp. to shut down its PlayStation Network for at least a week, disconnecting 77 million user accounts. 59 nations use the PlayStation network. Of the 77 million user accounts, about 36 million are in the U.S. and elsewhere in the Americas, 32 million in Europe and 9 million in Asia, mostly in Japan.

- **Stolen Data**
  - Account information, including names, birthdates, email addresses and log-in information was compromised for certain players.
  - Purchase history and credit card billing address information may also have been stolen but the intruder did not obtain the 3-digit security code on the back of cards.

- **Effects**
  - Hackers could use the stolen information to attempt to break-in to users other online accounts.
  - Stolen email addresses could be used to send official-looking messages filled with malware or directing users to dangerous Web links.

Sony

- **Possible Source & Motive**
  - Sony's CEO, Howard Stringer, indirectly implied that it was Sony's lawsuit with hacker George Hotz that incurred the wrath of hacker group Anonymous. On April 11, 2011 Sony stated it had reached a settlement with Hotz for posting a blog about how to play unlicensed games on the PlayStation 3. A week later, the first attack against Sony took place.
- **Outcome**
  - Some shareholders asked for Sony's CEO, Howard Stringer to step down.
  - Sony's stock had fallen 16% within the first month of the attack.
  - Sony's losses from the attacks may have totaled over $24 billion.
  - There was a restructuring of Sony Executives.

Sources:
"Sony Hacks: CEO Asked to Step Down by Shareholder, Refuses," June 28, 2011,TECHLAND http://techland.time.com/2011/06/28/sony-hacks-ceo-asked-to-step-down-by-shareholder-refuses/
"Sony claims exec shuffle unrelated to that little outage you may have heard about," June 30, 2011, IT WORLD http://www.itworld.com/it-managementstrategy/178935/sony-shuffles-execs-claims-it-has-nothing-do-little-outage-you-may-have

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 or contact the program at CSE@dhs.gov.

Cyber Security Evaluations for Critical Cyber Infrastructures

Cyber Security Evaluation Tool (CSET) v3

- CSET is designed to assess control system network security against recognized industry standards.
  - The current core of CSET standards include: *NIST 800-53, ISO/IEC 15408, NERC CIP-002, CIP-009, DoD Instruction 8500.2, and NIST 800-82*.
- It was developed under the direction of CSSP by cyber security experts with assistance from the National Institute of Standards and Technology (NIST).
- Self-applied or guided via DVD-based tool (~1 day to complete)

Cyber Resilience Review (CRR)

- CRR measures adoption and maturity aspects of cyber security risk management using a common, capability-based framework.
- CRR serves as a repeatable cyber review of an organization's ability to manage cyber security.
- CRR assists in constructive dialog and cooperative improvement.
- Expert-led via facilitated 5-6 hour discussion

Cyber Resilience Review (CRR)

- Goal: Assess how an organization manages cyber security during…
  - …normal operations (i.e., protection and sustainment)
  - …times of operational stress and crisis (i.e., survivability and resilience)

- Based on the CERT® Resilience Management Model (CERT-RMM) developed by Carnegie Mellon University's Software Engineering Institute [http://www.cert.org/resilience/rmm.html]

- The assessment addresses 4 key classes of cyber assets:
  - Information
  - Technology
  - People
  - Facilities

Cyber Resilience Review details

- The assessment is a 5-7 hour facilitated interview, typically including those who are responsible for cyber security management, IT operations, and business continuity of key services of the organization
- Topics are based on the CMU CERT®-RMM , and focus on cyber security management, including:

  - **Asset management**
  - **Vulnerability management**
  - **Service continuity**
  - **External dependency management**
  - **Incident management**
  - **Risk management**
  - **Information technology management**
  - **Situational Awareness**

- Assessment results will provide site-specific stakeholders with options for consideration to improve cyber security in support of critical infrastructure operations

Cyber Resilience Review

System-wide (i.e., Healthcare sub-Sector)

- Health Information Exchanges (HIE) records management
- Blood Bank messaging
- Field-Deployed Health IT and Delivery Systems

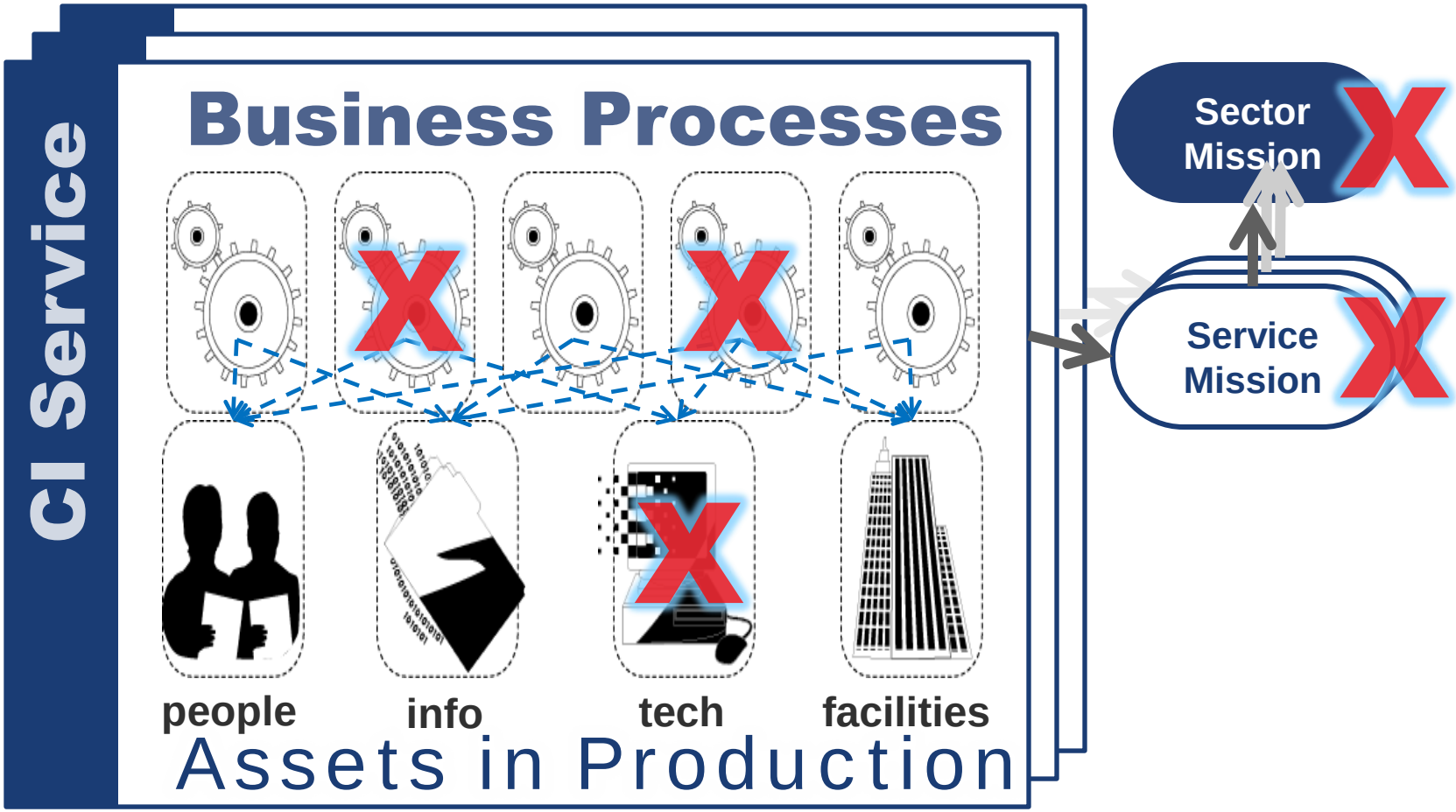
Multi-site CRR (i.e., 1x CIKR provider, Nx satellites)

- Corporate and operating unit disconnects (i.e., policy, procedural, etc)
- Incident management command-and-control
- Federate vulnerability analysis and reduction

Individual CRR (i.e., 1x CIKR provider)

- Specific Management Capabilities:
  - **Internal Cyber Security Management**
  - **External Dependency Management**
  - **Sector/Cross-Sector Cyber Security Alignment**
  - **National Cyber Security Alignment**
- Process Maturity:
  - **Can you repeat what you do successfully in times of stress?**
  - **Do you rely on a 'guy' / a 'gal' for the 'process'?**

“Critical infrastructure service” orientation



Cyber Resilience Score

- The CRR Report scores indicate relative strength for each key category
- A **Low Cyber Resilience Score** indicates:
  - Practices that are ad hoc or are not easily repeatable across the organization
  - Dependence on the skills, expertise, and heroic abilities of one or few people
  - Challenges to repeat practices, and no institutional knowledge about the execution of practice
  - Challenges to perform well under times of operational stress
- A **Medium Cyber Resilience Score** indicates:
  - Consistent, repeatable processes within the organizational unit related to establishing the process
  - Processes are not only stable and repeatable, but the output from each process can be reproduced with the same effectiveness regardless of who performs it
  - Categories and some practices are generally disconnected from other risk management activities,
  - Communicate and decisions based on some operational risk information; however, the ability to perform well under times of operational stress remains questionable
- A **High Cyber Resilience Score** indicates:
  - Consistent, repeatable processes across the entire organization
  - Processes are stable and repeatable and highly integrated with other repeatable processes
  - Objectives met by each process, as well as the integration requirement for individual processes, is understood and effectively communicated to all who need to know
  - Effective communication and decisions based on operational risk information, and is likely to perform well under times of operational stress

Options for Consideration

- The options for consideration aim to provide general guidelines or activities by which the organization can improve its cybersecurity posture
- The options for consideration focuses on improving cybersecurity management of services that support specific operational missions of the critical infrastructure organization
- The options for consideration are not meant to fully represent all activities needed for a robust cybersecurity management program, but to provide initial guidance on how to incorporate various cybersecurity practices, models, and standards, including:
  - CERT® Resilience Management Model (CERT-RMM)
  - National Institute of Standard and Technology (NIST) Special Publications (SP)

CRR Examples: Asset Management

Asset Management requires the process of identifying and defining assets by determining an asset's description, security requirements, ownership, sensitivity, and criticality. The organization should be able to identify the people, information, technologies, and facilities essential to delivering critical services. Asset-to-service traceability enables an organization to ensure that it develops appropriate protection and sustainability strategies that safeguard services vital to the Nation. Managing the impact of changes to assets ensures that protection and sustainability strategies are updated as appropriate.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Identify critical assets				• Established process to determine all critical cyber assets (CCAs) and supporting facilities • Mapping used to inform business continuity planning • Inventory not directly referenced in system security plans	• Consider automating the process of disabling access to critical assets a change in job responsibilities and roles occurs. • Consider classifying all assets related to the key service, once identified, according to the organization's sensitivity to the potential impact of their degradation, interruption, or loss.
Trace assets to services					
Identify asset protection & sustainability requirements					
Manage changes to assets					

CRR Results: IT Management

Information and Technology Management begins with the establishment of controls to support the confidentiality, integrity, and availability of the organization's information, as well as the integrity and availability of its technology. These attributes should be connected to the operational needs of the organization.

Practice	Score			Observations	Options for Consideration
	L	M	H		

Develop effective protection & sustainment strategies for IT assets				• Policies exist per operational group, but no common protection strategy
				• Operational risk management is an *ad hoc* tactical activity
				• Periodic training exists, but is not comprehensive
					• Consider establishing a training program that is tailored to those personnel with security responsibilities. Security training that is at a level commensurate with the responsibilities of personnel will help to ensure that the organization is consistently capable in this critical area of operations.
					  • NIST SP 800-16: IT Security Training Requirements
					  • CERT-RMM :
					  • OTA (Organizational Training and Awareness)
					  • KIM (Knowledge and Information Management)

Identify criteria for changing protection strategies					
Identify and mitigate operational risk					
Validate the function of security controls					
Ensure effective cyber security training and awareness					

CRR Results: Vulnerability Management

Vulnerability Management is the capability of the organization to formally identify, analyze, and manage vulnerabilities within assets and processes that support its critical services. Measurements in this area focus on plans, procedures, analyses, and communications as they apply to identifying and reducing vulnerabilities to critical services.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Establish a strategy to identify, analyze, and mitigate vulnerabilities				• *Ad hoc*, informal strategy; patch process applies mainly to Windows ® systems	• Consider developing vulnerabilities evaluation criteria specific to the needs of the organization. See NIST SP 800-42: Guideline on Network Security Testing. • Consider defining vulnerability management across operational areas and increasing the formal of linkage of Vulnerability Management to other related processes, such as Risk Management and Service Continuity Management.
Define evaluation criteria for vulnerabilities					
Perform vulnerability monitoring					

CRR Results: Incident Management

Incident Management is the capability of the organization to establish processes to identify and analyze incidents and to determine an appropriate organizational response. Measurements in this area focus on plans, procedures, analyses, and communications as they apply to detecting, responding to, and recovering from cyber incidents, which may negatively affect services.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Establish a repeatable and effective incident management process				• Incidents are automatically communicated to the business continuity planners • Alignment of IM criteria (to the role an asset plays in service delivery) is not formalized	• Consider incorporating incident management activities into organization-wide training and awareness for end users. • Consider increasing the formal of linkage of Incident Management to other related processes.
Define evaluation criteria for events and incidents					

CRR Results: Service Continuity

Service Continuity ensures the continuity of essential operations and related assets if a disruption occurs because of an incident, disaster, or other disruptive event. Measurements in this area focus on plans, procedures, and testing as they apply to managing continuity.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Prioritize essential services				• A process to identify and prioritize services is aligned to asset management and an asset 'tiering' structure identifies criticality of assets • A formal, repeatable service continuity process is in place that includes integration with key vendors	• Consider developing an After Action Review (AAR) process to measure the effectiveness of service continuity plans. AARs provide a means for identifying shortcomings and for improving the plan.
Develop effective continuity plans					

CRR Results: Environmental Control

Environmental Control establishes and manages the capability of the organization to identify and manage risk to assets that support the delivery of critical services from physical harm. Organizations should use their asset inventory to ensure they apply physical safeguards that align with organizational and sector needs. Measurements in this area focus on the identification and management of risk associated with facilities that contribute to securing and sustaining information and technology assets.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Prioritize facility assets				• Key facilities identified • Physical security controls in place • No strong connection between physical and logical security	• CERT-RMM Environmental Control (EC) process area, specific goals 2 and 3.
Assess physical risk and align that risk to the delivery of services					
Review and validate physical and environmental security strategies					

CRR Results: External Dependency

External Dependency Management ensures the resilience of services and assets that are dependent on the actions of third parties. When organizations establish operating relationships, they must identify and manage the risk of the failure of their operating partners. Measurements in this area focus on the identification and management of risk connected to such relationships, including suppliers, managed service providers, and other business partners that affect the delivery of services.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Identify dependencies on external parties				• Not integrated with other risk management processes • No formal or structured process • SLA's established • Public service dependencies integrated into continuity planning	• Consider developing and implementing a formal process to identify and evaluate the risk of external dependencies. This will ensure a more comprehensive and reliable level of analysis. For more information, please review NIST SP 800-39: Managing Risk from Information Systems. • CERT-RMM External Dependencies (EXD) Process Area Specific Goal 2.
Identify and reduce exposure to risk from dependant relationships					
Establish and review cyber security agreements with third parties					
Recognize and mitigate dependency on public services					

CRR Results: Situational Awareness

Situational awareness is the active discovery and analysis of information related to immediate operational stability and security and the coordination of such information across the enterprise to ensure that all organizational units are performing under a common operating picture. Measurements in this area focus on the active analysis and management of operational risk information as it applies to securing and sustaining information and technology assets that affect critical services.

Practice	Score			Observations	Options for Consideration
	L	M	H		
Learn about relevant, current cyber security information				• No formal process for threat awareness, and no subscription to any threat reporting services. • No formal process to evaluate trustworthiness of cyber security information sources • No pre-determined defensive cyber security activities defined against risk posture.	• Consider developing defensive and readiness strategies that could be implemented in response to heightened indications of threat. Examples of such strategies might include the limiting of new system deployments, the reduction of non-essential changes, and increasing monitoring efforts.
Evaluate sources of information for trustworthiness					
Define formal levels of readiness					
Establish a common operating picture					
Predict threats and events					

Benefits of the CRR

- CRR Report with options for consideration in key process areas
- Identification of process improvements to address cyber resilience
- Improved organization-wide awareness of the need for effective cyber security management
- One means of establishing a collaborative relationship between DHS and participants
  - Increased awareness and connecting participants with DHS cyber security programs and resources, such as:
    - Office of Cyber Security & Communications
    - US-CERT and ICS-CERT
    - Control Systems Security Program
    - Cyber Exercise Program
    - Training and education resources

Protected Critical Infrastructure Information (PCII)

- The results of your CRR may be categorized as PCII
  - http://www.dhs.gov/files/programs/editorial_0404.shtm

- The Protected Critical Infrastructure Information (PCII) Program is an information-protection program that enhances information sharing between the private sector and the government. The Department of Homeland Security and other federal, state and local analysts use PCII to Analyze and secure critical infrastructure and protected systems, Identify vulnerabilities and develop risk assessments, and Enhance recovery preparedness measures.

- If the information submitted satisfies the requirements of the Critical Infrastructure Information Act of 2002 , it is protected from The Freedom of Information Act (FOIA) ,State and local disclosure laws, and Use in civil litigation. PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements.

- Protected Critical Infrastructure Information (PCII) may be accessed by federal, state or local government employees and their contractors who meet the requirements of the PCII Program standard access policy. The copy of the critical infrastructure information (CII) that is retained by the submitter is not considered PCII. As such, it is not afforded the protections from disclosure under the Freedom of Information Act or similar State and local disclosure laws, and it is not subject to the PCII safeguarding, handling and access requirements

Observations: CIKR/State/Local Entities

- CSEP engages critical infrastructure and key resource (CIKR)owners and operators and State, Local, Tribal, Territorial, and Large Urban Area governments.
- Observations include:
  - 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.

Contact Information

Bradford Willke (bradford.willke@dhs.gov)
Mid-Atlantic Cyber Security Advisor
Deputy Director
+ 1 412-375-4069 (ofc)
+ 1 202-380-5899 (cell)
Cyber Security Evaluation Program
National Cyber Security Division
Office of Cyber Security and Communications

Homeland Security