Securing the Nation's Critical Cyber Infrastructure

Bradford J. Willke

FFRDC Liaison, Cyber Security Evaluations

National Cyber Security Division (NCSD)

April 14, 2010

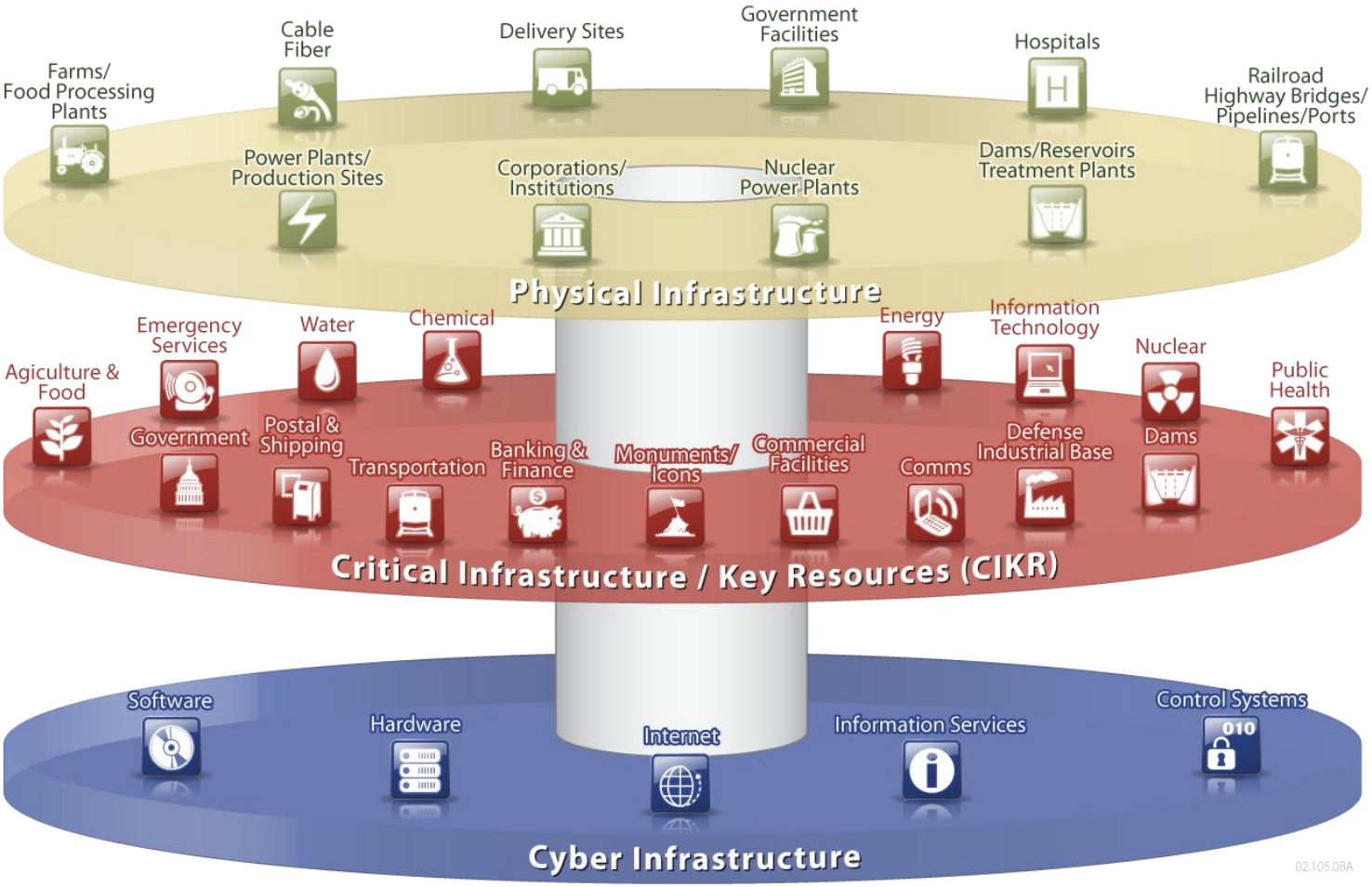
Homeland Security

Securing the Nation's Critical Cyber Infrastructure

- CIKR overview and reliance on the cyber infrastructure
- Understanding the cyber threats
- Addressing threats and risks to sectors
- Risk management and reduction

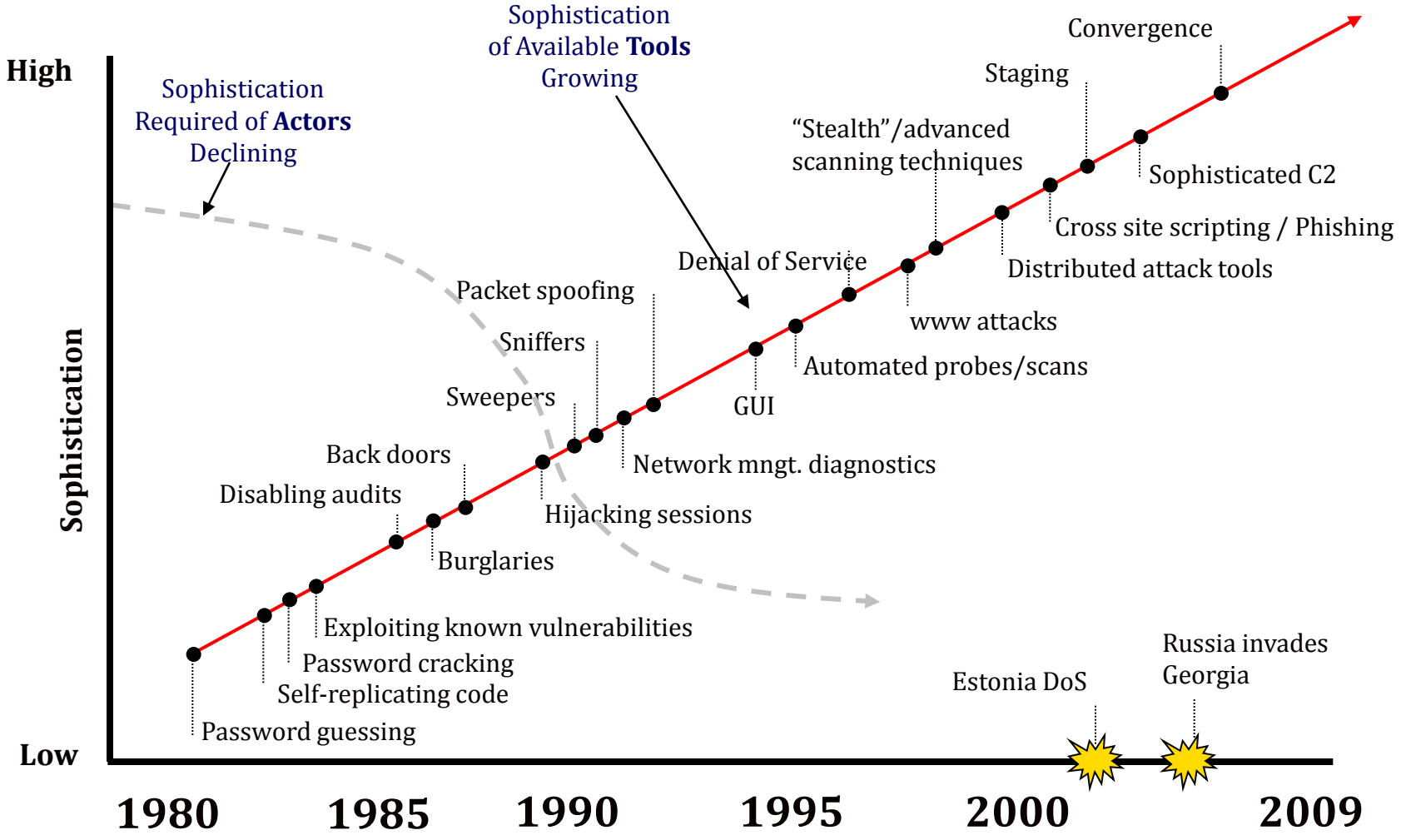
Homeland Security

CIKR Relies on Cyber Infrastructure



Homeland Security

Growth of Cyber Threats



Homeland Security

Securing the Nation's Critical Cyber Infrastructure

- CIKR overview and reliance on the cyber infrastructure
- Understanding the cyber threats
- Addressing threats and risks to sectors
- Risk management and reduction
- Program Overview and Initiatives

Homeland Security

Cyber Threat Actors

Cyber threats to federal information systems and cyber-based critical infrastructures… can come from a variety of sources, such as ***foreign nations*** *engaged in espionage and information warfare,* ***criminals****,* ***hackers****,* ***virus writers****, and* ***disgruntled employees*** *and* ***contractors*** *working within an organization.*

– Gregory C. Wilshusen,
Director, Information Security Issues
Government Accountability Office, 2009

Nation States

Criminals and Terrorists

Individuals

Homeland Security

Cyber Threat Actors: Nation States

We assess that a number of nations…have the technical capabilities to target and disrupt elements of the US information infrastructure and for intelligence collection. We expect disruptive cyber activities to be the norm in future political or military conflicts.

– Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence, 2009

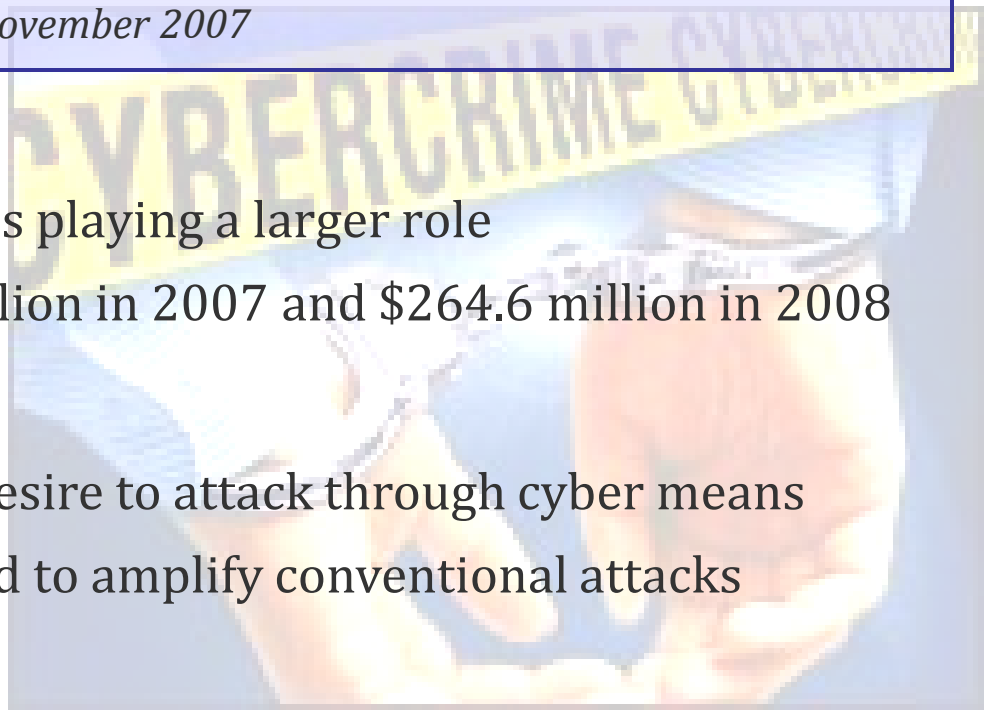
- Georgia, Estonia and Cyberwar
- Gaza, Whakerz of Pakistan, and Cyber Nationalism
- GhostNet and Cyber Espionage
- FBI has cited at least two dozen nations with an "aggressive interest" in penetrating US networks

Homeland Security

Cyber Threat Actors: Organizations

…the intersection between cyber crime and terrorism is becoming increasingly apparent. Cyber criminals and terrorists seek to harm our economy, our infrastructure, and our way of life.

– Robert S. Mueller, Director FBI
November 2007



Cybercrime

- Organized crime syndicates playing a larger role
- FBI: costs were $239.1 million in 2007 and $264.6 million in 2008

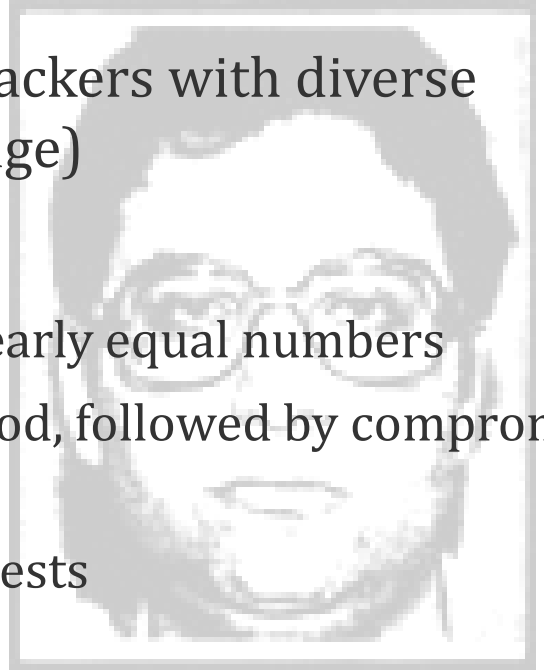
Cyberterrorism

- Groups have expressed desire to attack through cyber means
- Would most likely be used to amplify conventional attacks

Homeland Security

Cyber Threat Actors: Individuals

> The large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life.
>
> – US-CERT, Control Systems Security Program Website



Increased collaboration among individual hackers with diverse motives (Financial, Political, Prestige, Revenge)

The Insider Threat

- Current and former employees attacked in nearly equal numbers
- Social engineering is the most common method, followed by compromised accounts
- Roughly 38 percent of insiders have prior arrests

Homeland Security

Common Cyber Attack Methods

THREAT	DEFINITION	EXAMPLE
Zero Day Exploits	An exploit that takes advantage of a security vulnerability on the day it becomes known	December 2008 Windows XP/Server 2007: exploit creates an XML tag, crashes IE7, and runs malware when restarted
Spear Phishing	Attacks pinpointed at individual users to steal authentication and private data through e-mail, instant messaging, peer-to-peer networks, text messages, and VoIP	Nation States has been accused of sending deceptive mass e-mail messages to lure DOD users into clicking on malicious URLs
Botnets	Computers that are unknowingly controlled by a malicious individual or server	Estonian government websites were shut down after botnet-directed attacks
Compromised Websites	Hacker accesses backend database and takes advantage of input validation errors to redirect visitors to malicious sites	iFrameCash tool used by Russian Business Network and other cybercriminals

Homeland Security

Securing the Nation's Critical Cyber Infrastructure

- CIKR overview and reliance on the cyber infrastructure
- Understanding the cyber threats
- Addressing threats and risks to sectors
- Risk management and reduction

Homeland Security

Current Cyber Security Events

February 19, 2010

CRITICAL INFRASTRUCTURE PROTECTION:

- **Spike In Power Grid Attacks Likely In Next 12 Months:** Attacks against the power grid are likely to rise and intensify during the next 12 months as smart grid research and pilot projects advance, according to utility security experts and a recently published report that analyzes threats to critical infrastructure. The so-called Project Grey Goose Report on Critical Infrastructure points to state and/or non-state sponsored hackers from the Russian Federation of Independent States, Turkey, and China as the main threats to targeting and hacking into energy providers and other critical infrastructure networks. … The smart grid's distributed approach exposes these networks and systems,…and they will be most vulnerable in the early phases as they get up and running. … The worry is that smart grid vendors and energy firms are rushing to deploy the new technologies without properly securing them, utility security experts say. [Date: 19 February 2010; Source: http://www.darkreading.com/showArticle.jhtml?articleID=223000369]

February 21, 2010

GENERAL CYBER/ELECTRONIC CRIME:

- **Twitter users under attack again:** Security experts are warning Twitter users of yet another phishing attack aimed at stealing usernames and passwords. The malicious tweets in question take the form of a message… followed by a link including the term 'bzpharma.net' which leads to a fake user log-in page. Users entering their credentials on this fake site are shown a fake Twitter 'fail whale' before being taken back to the real Twitter main page. This means that they may not realise that their credentials have been compromised…. Twitter staff have said that the phishing messages are being sent by direct message only, but [Sophos senior technology consultant Graham] Cluley warned that they are also being posted in public fields. [Date: 21 February 2010; Source: http://www.v3.co.uk/v3/news/2258215/twitter-users-under-attack]

April 5, 2010

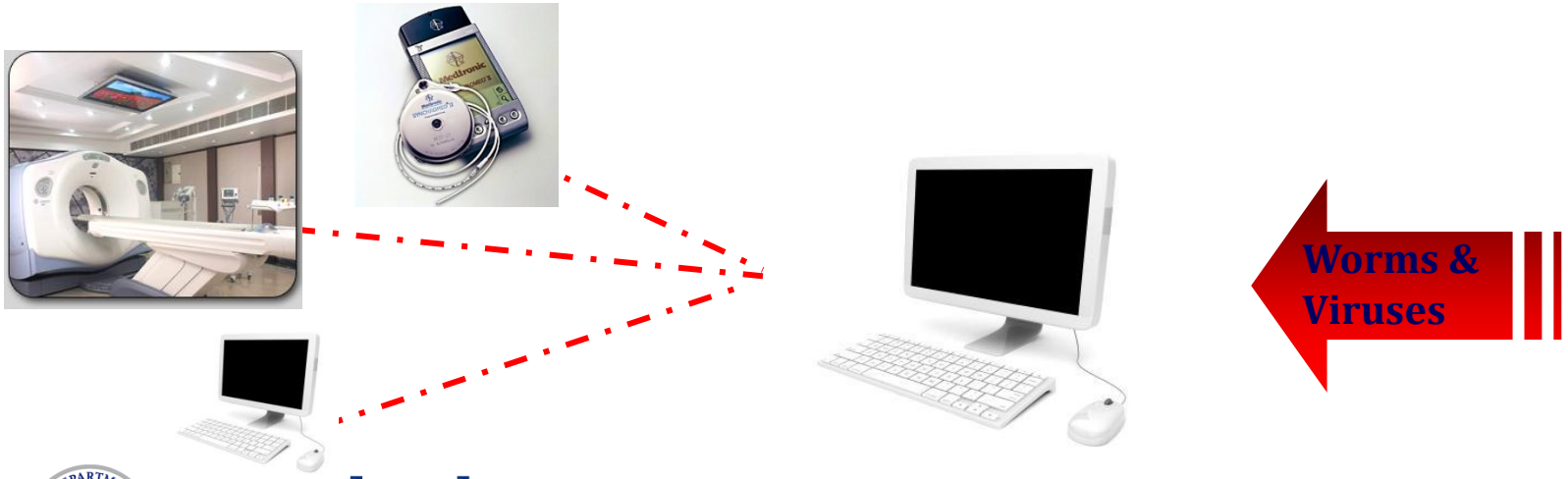
'Cyber Attack' Aimed At Texas Electricity Provider By Robert Arnold

Local 2 Investigates has uncovered details about a so-called "cyber attack" on one of Texas' largest electricity providers, KPRC Local 2 reported Saturday. A confidential e-mail obtained by Local 2 explains a "single IP address in China" tried 4,800 times to log in to the Lower Colorado River Authority's computer system. In the e-mail, the Electricity Reliability Council of Texas reports all login attempts failed and went on to term the incident a "suspected sabotage event." The e-mail explained the FBI had been notified. "NERC evaluates all reported incidents, and works with the entity and our stakeholders and government partners," the company wrote in a statement. "This incident demonstrates the value of information sharing and highlights the ability of this utility to identify directed malicious probes and work with partners to properly enhance their defenses. Utilities must remain vigilant and aware of attacker techniques to constantly evaluate the security of their systems." http://www.click2houston.com/news/23046216/detail.html

Homeland Security

Healthcare and Public Health Specifics

- Medical Device Vulnerabilities
  - The Conficker virus has infected important computerized medical devices (Pacemakers) through wireless and other LAN connections
- Integrity of Electronic Medical Records:
  - Computerized hospital records may be accessed through interconnected systems (hospitals, emergency care facilities, doctors offices)
  - Portability and transferability of patient records on PDAs and



Homeland Security

Energy Sector Specifics

- Potential Threat Vectors: Automated Equipment
  - Electricity infrastructure is highly automated and controlled by utilities and regional grid operators who rely on energy management systems
  - SCADA systems and other protected energy systems that were standalone are not connected to corporate and other networks
- Knowledge of Cyber Risks
  - Energy asset owners and operators still do not have the capabilities to fully understand the risks associated with the cyber threats of today and tomorrow as threats are constantly evolving
  - Difficult to keep pace with the rapidly changing and growing threat environment

Homeland Security

Communications: highly interconnected industry - many transmission systems

Dams: 82,642 dams in the US

Food & Agriculture: *2.1 million farms, 880,500 firms, million facilities*

Defense Industrial Base: geographically dispersed, critical systems

Water: *160,000 public drinking water systems and over 16,000 wastewater treatment systems*

Transportation: *450 commercial airports, railroads, daily commuters*

National Monuments & Icons: *government owned, resources undergo C&A*

Cyber Infrastructure

All critical infrastructure rely on cyber infrastructure

Health Care & Public Health: *reliance on technology: electronic health records, and medical devices*

Postal & Shipping: *over 300 high-volume automated processing facilities; 50,000 transport vehicles; information networks*

Critical Manufacturing: *production highly dependent on control systems*

Nuclear: 21% of the US electric produced from 104 power plants

Energy: *284 billion miles of crude pipelines*

Emergency Services: *law enforcement, fire and rescue, emergency medical services (EMS), and emergency management personnel*

Chemical: *over 7,000 high-risk chemical facilities*

Government Facilities: *Protection of data and resources*

Banking and Finance: *8% of US Gross Domestic product*

Information Technology: *critical domain name resolution services*

Commercial Facilities: 35 million US workers in office buildings

Securing the Nation's Critical Cyber Infrastructure

- CIKR overview and reliance on the cyber infrastructure
- Understanding the cyber threats
- Addressing threats and risks to sectors
- Risk management and reduction

Homeland Security

Response to Cyber Threats: DHS Cybersecurity and Communications

Mission: Prepare for and respond to catastrophic incidents that could degrade or overwhelm the networks, systems, and assets that operate our Nation's IT and communications infrastructure

National Cyber Security Division	Office of Emergency Communications	National Communications System
Works collaboratively with public, private, and international entities to secure cyberspace and America's cyber assets	Integrates and coordinates Government-wide efforts addressing interoperable emergency communications	Works with the public and private sectors to ensure continuity and restoration of communications for the Nation in times of domestic emergencies

Homeland Security

CSE Program Initiatives

Major CSE functional initiatives include:

- Promote cyber security across the 18 CI/KR Sectors
- Mitigate the risk from globalization
- Collaborate with the Intelligence Community on cyber threats
- Work with State and local government and jurisdictions to secure cyber assets
- Providing solutions to mitigate cyber risk

The United States is the most vulnerable nation on Earth to cyber attack.

– J. Michael McConnell,
Former Director of National Intelligence, 2008

Homeland Security

Cyber Security Assessments

Improve the security posture of CIKR, State and Local governments, and international partners through on-site assessment activities

Cyber Resilience Review (CRR)

- Measures and enhances the implementation of key cyber security capacities and capabilities of critical infrastructure and key resources
- Comprehensively assesses the overall practice, integration, and health of the organization's cyber security program
- Ensures that core process-based capabilities exist, are measureable, and are meaningful
- Creates a forum for the discovery and exchange of protective cyber strategies with information security leadership from critical infrastructure
- Identifies opportunities for improvement in cyber security management and reduce operational risks related to cyber security

Homeland Security

Cyber Resilience Review

CRR Assessment Overview

- A Pre-Assessment questionnaire consisting of 15 high level questions will be sent out in advance in order for our team to gain an initial understanding of the site
- CRR will take approximately a 6 – 8 hours to complete on – site; the length of the assessment is dependant on a set of principle questions

Identifies and measures the Resilience of CIKR participants to manage cyber security within nine (9) key process areas:

- Asset Definition and Management
- Environmental Control
- Communications Management
- Service Continuity
- Technology Management
- External Dependency
- Incident Management and Control
- Situational Awareness
- Vulnerability Analysis and Resolution

Homeland Security

Cyber Resilience Review

Goal/Practice	Level of Capability		
	Low	Medium	High
Ability to Inventory and Establish Critical Assets	----------X----------		
Ability to Communicate a Common Understanding of Critical Assets	----------X		
Ability to Analyze Dependencies Between Assets	----------X-------		
Ability to Maintain Changes to Assets	----------X-------		

Sample Questions:

1. Asset Management – Does the organization trace people, information, technology, and facility assets to (national) critical infrastructure operations and services?

2. Incident Management – Does the organization have a formal process for monitoring, identification, and reporting of events?

Sample Expected Evidence:

1. Asset Management – List of high services and associated assets; asset profiles; inventory databases and records

2. Incident Management – Procedures defining incident identification and handling; vendor contracts; incident management policy; event/incident escalation criteria; help desk

Homeland Security

Cyber Resilience Review

Benefits of a CRR:

- Site will receive a full report detailing the cyber security capability assessment of the facility
- Participants gain insight into their cyber security management, how cyber security supports essential organizational missions and functions, and results can serve as a guidepost for organizational improvement
- Capture information to be analyzed in conjunction with other site information and create picture of Resilience
  - Options for consideration for improving cyber security in support of critical infrastructure operations
  - Documentation of capabilities and capacities to include strengths, weaknesses, opportunities, threats

Cyber Resilience Review

Lessons-Learned

- Technology agnosticism
- Process measurement
  - What over How
- Dependency and interdependency

Case Study Results

- Services → Assets → Systems of Interest → Component (traceability)
- Asset management and communications are foundational
- Internal and external dependencies exist
- Situational awareness remains illusive

Homeland Security

Nationwide Cyber Security Review

- House Report 111-298 states the following requirement:
  - The National Protection and Programs Directorate (NPPD), in cooperation with FEMA and relevant stakeholders, shall develop the necessary tools for all levels of government to complete a cyber network security assessment so that a full measure of gaps and capabilities can be completed in the near future
- Per the conference report language, CSE has made the assumption that 50 States and 62 large urban areas comprise the full scope of assessments.
- Stakeholders include:
  - Multi-State Information Sharing and Analysis Center (MS-ISAC)
  - National Association of State Chief Information Officers (NASCIO)
  - FEMA
  - NPPD
  - Protective Security Advisors

Homeland Security

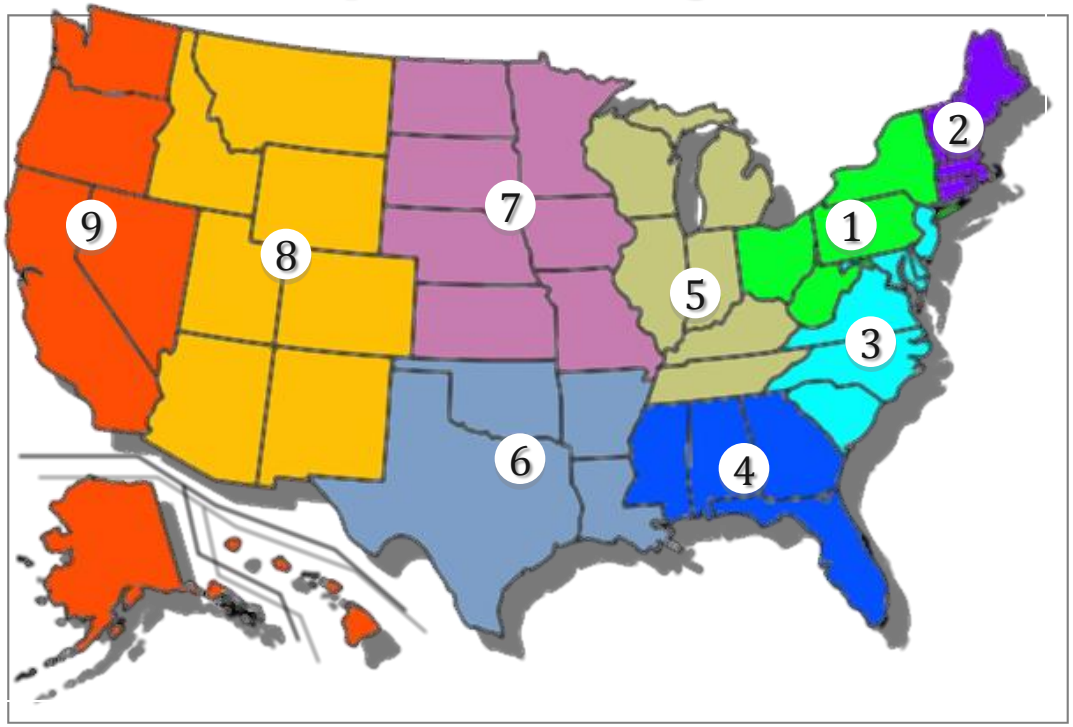
Cyber Security Advisor Pilot

- Manage and conduct cyber risk and vulnerability evaluations of planned and installed cyber systems, networks, and infrastructures supporting CI/KR operations, including site-specific and regional Resilience assessment projects

Proposed CSA Responsibilities

1. Provide Regional Cyber Security Support
2. Establish and maintain a close working relationship with Federal, State, territorial, local, and tribal, and private industry cyber security officials
3. Plan, analyze, develop, implement, maintain, and enhance cyber security evaluation tools
4. Serve as an additional capability within Fusion Centers that focuses on securing the Nation's CIKR

Proposed CSA Regions



Homeland Security

Other Partnerships and Initiatives

- Help Protective Security Advisors coordinate cyber awareness requests with CIKR asset owners and operators
  - Participating in the RRAP and SAV process by providing cyber security assessment module
- Work closely with state, local, tribal, and territorial partners through the National Association of State Chief Information Officers and other bodies to ensure participation in National CIKR protection efforts

Homeland Security

Homeland Security

Contact Information

Bradford J. Willke (bradford.willke@dhs.gov) 412-268-5050

FFRDC Liaison, Cyber Security Evaluations

National Cyber Security Division

Office of Cybersecurity and Communications

Homeland Security