Coordinating and Guiding Federal, State, and Private Sector Cybersecurity Initiatives

Seán Paul McGurk, Director
Control Systems Security
U.S. Department of Homeland Security
How do we define Cyberspace?

- Cyberspace is composed of hundreds of thousands of globally interconnected computers, servers, routers, switches, and cables that allow the critical infrastructures to work.
  - It transcends physical, organizational and geopolitical boundaries and thus has global stakeholders from both the public and private sectors.

- It encompasses the logical layer where software applications, Web sites, bulletin boards, chat rooms, e-mail, and electronic exploits (e.g., viruses, Botnets, etc) operate.

- While the Internet is part of cyberspace, it also includes the local and wide area networks, as well as the users connected to the Internet.

- These networks contain a wealth of information that includes proprietary, classified and private data and operate many of the nation’s critical infrastructure and key resources.
Comprehensive National Cybersecurity Initiative Goals

• To establish a front line of defense against today’s immediate threats by creating or enhancing shared situational awareness of network vulnerabilities, threats, and events within the Federal Government—and ultimately with state, local, and tribal governments and private sector partners—and the ability to act quickly to reduce our current vulnerabilities and prevent intrusions.

• To defend against the full spectrum of threats by enhancing U.S. counterintelligence capabilities and increasing the security of the supply chain for key information technologies.

• To strengthen the future cybersecurity environment by expanding cyber education; coordinating and redirecting research and development efforts across the Federal Government; and working to define and develop strategies to deter hostile or malicious activity in cyberspace.
## Comprehensive National Cybersecurity Initiative

<table>
<thead>
<tr>
<th>Trusted Internet Connections</th>
<th>Deploy Passive Sensors Across Federal Systems (Einstein 2)</th>
<th>Pursue Deployment of Intrusion Prevention System (Einstein 3)</th>
<th>Coordinate and Redirect R&amp;D Efforts</th>
</tr>
</thead>
<tbody>
<tr>
<td>(reduce and consolidate external access points)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Establish a front line of defense

<table>
<thead>
<tr>
<th>Connect Current Cyber Centers to Enhance Cyber Situational Awareness (National Cyber Security Center)</th>
<th>Develop Government Wide Cyber Counterintelligence Plan</th>
<th>Increase the Security of the Classified Networks</th>
<th>Expand Education</th>
</tr>
</thead>
</table>

### Demonstrate resolve to secure U.S. cyberspace & set conditions for long-term success

<table>
<thead>
<tr>
<th>Define and Develop Enduring Leap Ahead Technology, Strategies &amp; Programs</th>
<th>Define and Develop Enduring Deterrence Strategies &amp; Programs</th>
<th>Develop Multi-Pronged Approach for Global Supply Chain Risk Management</th>
<th>Define the Federal Role for Extending Cybersecurity into Critical Infrastructure Domains</th>
</tr>
</thead>
</table>

### Shape the future environment to demonstrate resolve to secure U.S. technological advantage and address new attack and defend vectors

*Homeland Security*
Authorities in Cyberspace

Law Enforcement Networks

Military Networks

Intelligence Networks

Government Networks
DHS Cybersecurity Organizations

**Department of Homeland Security**
- Improves our nation’s readiness for natural disasters in terms of preparedness, response and recovery
- Guards against terrorism
- Provides assessments of physical and cyber threats to critical infrastructure (Intelligence and Analysis Directorate)
- Safeguards the payment and financial systems of the U.S. by investigating crimes involving computer and telecommunications fraud (U.S. Secret Service)

**National Protection and Programs Directorate**
- Reduces security risks across both physical and cyber infrastructure as well as telecommunications
- Oversees the Departments CNCI efforts

**National Cybersecurity Center**
- Coordinates and integrates information across the interagency (.mil, .gov, and .ic domains) to develop strategic reporting as well as mitigation strategies based on identified risks

**Cybersecurity and Communications**
- Ensures the security, resiliency and reliability of the nation’s cyber and communications infrastructure

**National Cybersecurity and Communication Integration Center**
- Builds and maintains an effective national cyberspace response system
- Implements a cyber-risk management program for protection of critical infrastructure
- Provides response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) through:
  - Information sharing and coordination
  - Alert, warning and analysis,
  - Response and assistance
Vision

• The NCCIC incorporates the interrelated missions of the following organizations to prevent, protect and respond to threats and incidents affecting the national information and communications infrastructure:
  – National Communications System (OMNCS), National Coordinating Center (NCC)
  – National Cyber Security Division (NCSD), United States Computer Emergency Readiness Team (US-CERT)
  – National Cyber Security Division (NCSD), Industrial Control System Cyber Emergency Response Team (ICS-CERT)
  – Office of Intelligence and Analysis (I&A)
  – National Cybersecurity Center (NCSC)
  – Department and Agency Security Operations Centers
  – Law Enforcement and Intelligence Community Representatives
  – Private Sector

• The NCCIC supports the overall cyber mission of DHS by:
  – Providing support to the decision making process for the Federal Government;
  – Enabling incident response through shared situational awareness; and
  – Supporting the missions of components.
Components of the NCCIC

- NCCIC is comprised of organizational components and operational liaisons.
  - *Components* refers to DHS organizations that have a major presence on the NCCIC floor, such as US-CERT, NCC, NCSC, and I&A
  - *Operational Liaisons* refers to representatives from the federal departments and agencies, intelligence community, law enforcement, and private sector that participate in the NCCIC physically and/or virtually.

- While each component maintains their own operating mission, the execution of NCCIC’s mission relies on coordinated operations that contribute to all products and services.
Cyberspace Threat Vectors

**Threat Level 1**
“Garden Variety”
- Inexperienced
- Limited funding
- Opportunistic behavior
- Target known vulnerabilities
- Use viruses, worms, rudimentary trojans, bots
- Acting for thrills, bragging rights
- Easily detected

**Threat Level 2**
“Mercenary”
- Higher-order skills
- Well-financed
- Targeted activity
- Target known vulnerabilities
- Use viruses, worms, trojans, bots as means to introduce more sophisticated tools
- Target and exploit valuable data
- Detectable, but hard to attribute

**Threat Level 3**
“Nation State”
- Very sophisticated tradecraft
- Foreign intel agencies
- Very well financed
- Target technology as well as info
- Use wide range of tradecraft
- Establish covert presence on sensitive networks
- Difficult to detect
- Supply Interdiction/hardware implants
Cyber Threat Profile

The Threat

- The threats are large and diverse, ranging from independent, unsophisticated, opportunistic hackers to very technically competent intruders and nation states using state-of-the-art intrusion techniques.

- Malicious actors are increasingly acquiring information technology skills to launch malicious attacks designed to steal information and disrupt, deny access to, degrade or destroy critical information and infrastructure systems.

- Hacker groups already possess the necessary skills to launch a successful cyber attack and may be “talent-for-hire” available to terrorist, criminal organizations, and nation states.

- Attackers do not need to be technically savvy as free and commercial automated tools are simplifying attack methods.

- Both actors and system vulnerabilities put infrastructure at risk.

Reliance on Cyberspace

- Society increasingly relies on technology and telecommunications to support our economy and business operations and critical functions of government.

- Global wireless and cellular usage is on the rise.

- To put individual demand in perspective,
  - 1.5 billion individuals currently utilize the Internet and this number is growing.
  - Over 200 billion emails are sent per day.
  - 8 hours of YouTube are uploaded every minute.
Each day news stories illustrate that cyber incidents are increasing in frequency, scale, and sophistication.

Hackers Update Conficker Worm, Evade Countermeasures
Gregg Keizer, Computerworld
Tuesday, March 10, 2009 7:17 AM PDT
Computers infected with the Conficker worm are being updated with a new variant that sidesteps an industry effort to sever the link between the worm and its hacker controllers, researchers at Symantec Corp. said Friday.

Government computers under attack
Greg Masters February 17, 2009
Records show that cyberattacks on federal computer networks increased 40 percent last year, and that figure is likely lower than the reported attack.

Based on data provided by US-CERT, unauthorized access and installations of hostile programs rose from a combined 3,928 incidents in 2007 to 5,444 in 2008.

From Times Online
August 11, 2008
Georgia accuses Russia of waging 'cyber-war'
Several Georgian state websites have been affected by Russian hackers, though the extent of the attacks remains unclear.

TJX theft tops 45.6 million card numbers
Robert Lemos, SecurityFocus 2007-03-30
More than three months after detecting a breach of its systems, retail giant TJX Companies released this week its best guess at the number of customers whose credit-card information and other data were stolen by online thieves.

Information from at least 45.6 million credit cards had been stolen by unknown attackers who had breached the company's computer transaction processing systems between July 2005 and mid-January 2007, TJX stated in its annual report.
Cyber systems are essential national and economic security, and the provision of critical government functions and services.

- Cyber Infrastructure, which represents the convergence of information technology and communications systems, is inherent to nearly every aspect of modern life.

Illustrative examples only -- not all inclusive
Rail Transportation

Event: January 2008, A Polish teenager modifies a TV remote and hacks Lodz Tram system

Impact: 12 people injured, 4 derailments

Specifics: The 14-year-old modified a TV remote control so that it could be used to change track points. Local police said the youngster trespassed in tram depots to gather information needed to build the device. The teenager told police that he modified track setting for a prank.

Lessons learned:
- Do not rely on protocol obscurity for security
- Apply appropriate access controls to all field devices
Event: Feb, 2009 Italian authorities investigating unauthorized changes to traffic enforcement system

Impact: Rise of over 1,400 traffic tickets costing > 250K Euros in two month period

Specifics: Engineer accused of conspiring with local authorities to rig traffic lights to have shorter yellow light causing spike in camera enforced traffic tickets

Lessons learned:
- Do not underestimate the insider threat
- Ensure separation of duties and auditing
**Event**: July 28, 2009, Duke Energy in Cincinnati OH sends incorrect signal sent to 18,000 air condition units.

**Impact**: 18,000 households participating in Duke Energy's energy saving program for three hours.

**Specifics**: An erroneous message was broadcasted by Duke Energy that shut down 18,000 households for three hours. Human error was the blame for the incident and all units were restored by 8:30 pm.

**Lessons learned**:
- Consider all design parameters when implementing broad control. (load shedding versus peak load conservation)
- Identify controls to minimize human error.
Smart Meters

Event: October 2009

Impact: Altered “SmartGrid” electric meters discovered

Specifics: Spot checks discovered approx 10% of meters checked were altered by methods that included changing the meter’s software settings.

Meters were altered for various costs, depending on the meter model.

Meters reported less consumption, and reduced electricity bill by one half or three quarters.

Lessons learned:
- Do not rely on protocol obscurity for security
- Apply appropriate access controls to all field devices
- Do not underestimate the financial motivation
SCADA Server accessed via Internet

Event: January 2010 - Cyber researcher used new search engine “SHODAN” to identify an online link to a utility company’s SCADA system. The system was then accessed using the default user name and passwords.

Impact: None, the researcher only “looked around,” but touched nothing.

Specifics: Key word internet searching revealed the default information.

Lessons learned:
- Change system default user names and passwords
- Avoid posting system details to public facing devices
- Not all public facing system details are obviously visible
Searching for SCADA in SHODAN
SHODAN devices labeled “SCADA”
One Device has SCADA Web Login
Searching for Default Vendor Credentials
User accesses system with ‘ADMIN’ rights
User accesses system with ‘ADMIN’ rights
‘Safe Harboring’ using ICS systems

**Event:** Foreign hacker penetrated security at a water filtering plant

**Impact:** The intruder planted malicious software on the industrial control network which remained undetected by the enterprise network security systems

**Specifics:** The infection occurred through the Internet and did not seem to be an attack that directly targeted the control system

**Lessons learned:**
- Secure remote computers
- Defense-in-depth strategies, Firewalls & Intrusion Detection Systems
- Critical patches and Anti-virus needs to be applied and updated regularly
Interdependencies between physical and cyber infrastructures can lead to cascading effects in an attack or catastrophic event.
The National Cyber Security Division (NCSD) is the federal government’s lead agency for assessing, mitigating and responding to cyber risks in collaboration with public and private sectors.

**Mission**
To work collaboratively with public, private, and international partners to secure cyberspace and America’s cyber infrastructure.

**Goals**
- Manage cyber risk to the nation and integrate cybersecurity into public and private sector efforts;
- Maintain and enhance national cyber response capabilities; and
- Build and maintain a world-class organization to advance the nation’s cybersecurity preparedness, and raise awareness across the Nation on cybersecurity.
The US-CERT is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) as well as information sharing and collaboration with State and local government, industry and international partners.

- **Operational readiness and mitigation:** Leads efforts in response to cyber activity for the (non-Department of Defense and Intelligence) Federal Executive Branch cyber infrastructure.

- **Alert, Warning, and Analysis:** Detects, compiles, analyzes and shares information about cyber incidents.

- **Response and Assistance:** Providing timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents.
Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)

Protecting Our Nation’s Critical Infrastructure

- Providing situational awareness in the form of actionable intelligence
- Conducting vulnerability and malware analysis
- Responding to and analyzing control systems related incidents
- Partnering with the federal, international, and private sector to secure systems
Partnership

Law Enforcement and First Responder Communities

Private Sector

Department of Homeland Security
National Cyber Security Division

Federal Departments and Agencies

State and Local Governments
Developing a Strong Cybersecurity Posture

PUBLIC SECTOR

Lacks…

- A qualified cyber workforce
- Recruitment and retention of qualified personnel
- A comprehensive training and education curricula for the current cyber workforce
- Enhanced awareness of cyberspace
- Enforcement authority to combat cyber crime and industrial espionage.
- Sufficient information sharing between departments and agencies
- Agreement with the private sector on the way forward
- A common cyber language

PRIVATE SECTOR

Lacks…

- A comprehensive understanding of cyber threats and vulnerabilities
- An established relationship with the public sector to determine the way forward
- Sufficient information sharing among private corporations

Need to increase collaboration and information sharing between the public and private sectors
In 2009, the DHS’ National Cyber Security Division (NCSD) issued the **Strategy for Securing Control Systems**, which focuses on the vision and elements necessary for coordinating activities to improve control systems security in the nation’s critical infrastructures.

As the lead federal agency involved in industrial control systems cybersecurity for Critical Infrastructure and Key Resources (CIKR), NCSD continues to coordinate security efforts among stakeholders across critical infrastructure sectors.
Web Based Training

- “Cyber Security for Control Systems Engineers and Operators”
- “Operational Security (OPSEC) for Control Systems”*

Instructor Led Courses

- Introduction to Control Systems Security for the Information Technology Professionals
- Intermediate Control Systems Security
- Cyber Security Advanced Training and Workshop

International Training

- 30 countries have participated
- Provided basic, intermediate and advanced training

*IOSS first place award 2008
The Way Forward

• Incentivize recruitment and retention of qualified workforce
• Promote/integrate new partnerships within cyber related exercises
  – E.g. Cyberstorm III
• Improve cyber awareness with state, local and tribal governments
• Increase information sharing between the public and private sector
• Increase information sharing and communications with our international partners