



The Federal Government Role in Cyber Security

Jeanie M. Larson, CISSP-ISSMP, CISM

Jeanie.Larson@yahoo.com

October 29, 2009

DISCLAIMER: Everything represented in here is the opinion of the speaker. The speaker is not representing the United States Government.

What Will be Covered Today

- Summary of events leading up to the proposed creation of a Cyber Office
- Summary of Reports Driving Policy Changes
- Where will the Cyber Office reside?
- Authorities and Lines of Authority in the USG – clarification of roles
- Does this effort pose risks to privacy on the Internet or other networks?
- What safety can we expect to gain from this appointment?
- Will there be more legislative action to support this effort?

Opinions and Disclaimers

The opinions expressed in this material are solely my own and do not represent the opinions or views of my employer(s) past or present.

Jeanie M. Larson

Spelling and Terms

Throughout this document, you will find two phrases used synonymously

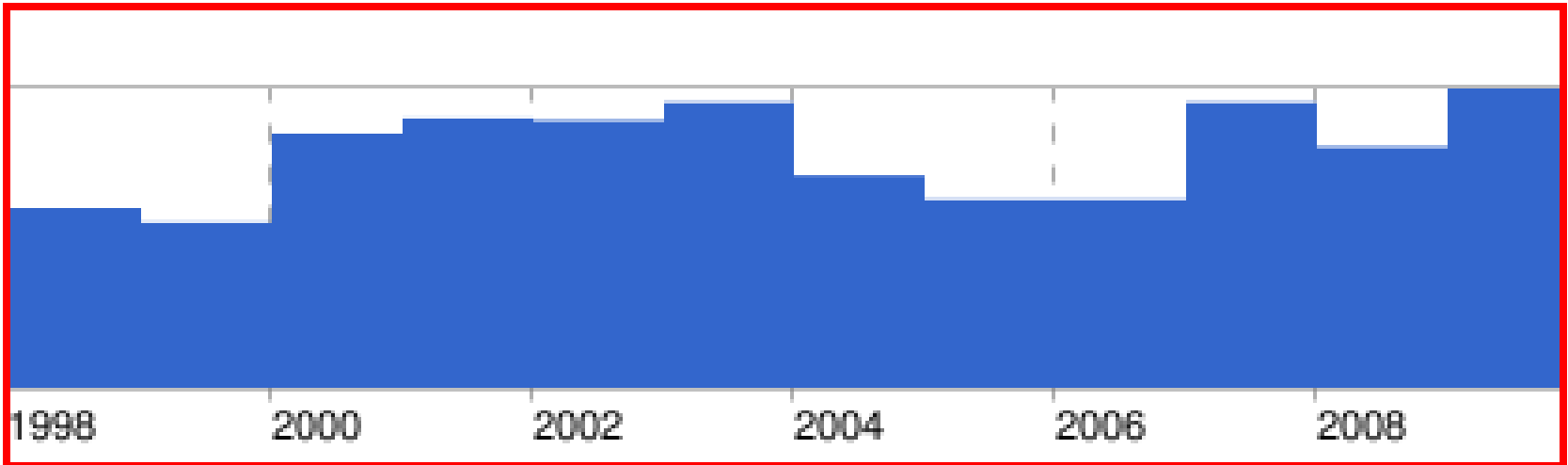
- 1) Cybersecurity
- 2) Cyber Security

ACRONYMS – used throughout this document are spelled out. Reference links to additional information are included at the end of this presentation for those interested in more details.

Events Leading up to the Cyber Czar



Timeline of Key Cyber Events



Attacks

September 1999 – Moonlight Maze

July 2001 – Code Red

September 2001 – NIMDA

The Invasion of the Chinese Cyber Spies (And the Man Who Tried to Stop Them)

By Nathan Thornburgh/Washington Monday, Aug. 29, 2005

April 2007 – Cyber attacks crippled Estonia's network coinciding with the relocation of the Bronze Soldier of Tallinn

August, 2008 – Then Senator Barack Obama and Joe Biden's campaign computers

<http://www.time.com/time/nation/article/0,8599,1902073,00.html?iid=sphere-inline-sidebar>)

July 2009 – Cyber attacks targeting the United States and South Korea (DDoS)

Moonlight Maze

Moonlight Maze refers to a highly classified incident in which U.S. officials accidentally discovered a pattern of probing of computer systems at the Pentagon, NASA, Energy Department, private universities, and research labs that had begun in March 1998 and had been going on for nearly two years. Highly placed sources told FRONTLINE that the invaders were systematically marauding through tens of thousands of files -- including maps of military installations, troop configurations and military hardware designs. The Defense Department traced the trail back to a mainframe computer in the former Soviet Union but the sponsor of the attacks is unknown and Russia denies any involvement. Moonlight Maze is still being actively investigated by U.S. intelligence.

July 2001 - Code Red

Code Red was a worm with multiple variants that first appeared in July 2001 and ultimately affected nearly 300,000 computers in the U.S. Exploiting a hole in Microsoft's IIS Web servers, it was time sensitive based on the date: From days 1-19 of the month the worm would propagate; from days 20-27 it would launch a denial of service attack against a particular site, and from day 27 through the end of the month the worm would "sleep," dormant in the computer. In Code Red's first variation, the affected computers were programmed to launch a denial of service attack against the White House Web site at a certain date and time. If the assault worked, the hundreds of thousands of pings would have overwhelmed the Internet in nanoseconds. [Richard Clarke](#), the president's adviser for cyberspace security, worked with the nation's Internet providers to thwart the attack by blocking traffic to the White House site. Other Web sites were shut down, however, and replaced by a message that read "Hacked by Chinese."

2001 - Mountain View

In the summer of 2001, the coordinator for the city of Mountain View, Calif.'s Web site noticed a suspicious pattern of intrusions. The FBI investigated and found similar "multiple casings of sites" in other cities throughout the U.S. The probes were seemingly emanating from the Middle East and South Asia, and the visitors were looking up information about the cities' utilities, government offices, and emergency systems. This information took on a new significance when U.S. intelligence officials examined computers seized from Al Qaeda operatives after the Sept. 11 attacks and discovered what appeared to be a broad pattern of surveillance of U.S. infrastructure.

September 2001 - NIMDA

The Nimda worm ripped through the U.S. financial sector one week after the Sept. 11, 2001 terrorist attacks. Nimda, which is "admin" spelled backwards, was a mass-mailing worm that exploited vulnerabilities in Microsoft software. It was notable because of its sophistication. It could replicate itself several ways -- by infecting e-mail programs, copying itself onto computer servers, or afflicting users who downloaded infected Web pages. Nimda was also significant for its speed and potency -- it affected millions of computers and slowed the Internet. Officials do not believe it was related to the Sept. 11 attacks.

January 2003

Slammer Worm aka Sapphire Worm

Super bowl Weekend 2003:

- Exploit MS SQL Server 2000
- Fastest cyber attack in history (doubling ever 8.5 seconds!)
- 90% of damage occurred in the first 10 minutes after its release

2003 – Titan Rain

Beginning in 2003 (as far as we know)

Attacks continue...

Sophisticated, undetectable by “best practices”
implementation of protection infrastructure:

- Anti-Virus (less than 25% of these detected)

- Firewall

- Content Filtering – Can detect very few attacks

- Intrusion Detection/Prevention

Perimeter Protection Ineffective

- Attacks originate from “inside” the perimeter

February 2007 –DNS Root Servers Attacked

On 6 February 2007, starting at 12:00 pm UTC (4:00 am PST), for approximately two-and-a-half hours, the system that underpins the Internet came under attack. Three-and-a-half hours after the attack stopped, a second attack, this time lasting five hours, began.

The core DNS servers of the Internet were hit with a significant distributed denial of service attack, or DDoS. In such an attack, billions of worthless data packets are sent from thousands of different points on the Internet to specific computer servers in order to overwhelm them with requests and so disrupt the smooth running of the Internet.

At least six root servers were attacked but only two of them were noticeably affected: the “g-root”, which is run by the U.S. Department of Defense and is physically based in Ohio, and the “l-root” run the Internet Corporation for Assigned Names and Numbers (ICANN), which is physically based in California.

January 2008 – Cyber Attack Caused Multi-City Power Outage

SANS FLASH

CIA Confirms Cyber Attack Caused Multi-City Power Outage

On Wednesday, in New Orleans, US Central Intelligence Agency senior analyst Tom Donahue told a gathering of 300 US, UK, Swedish, and Dutch government officials and engineers and security managers from electric, water, oil & gas and other critical industry asset owners from all across North America, that "We have information, from multiple regions outside the United States, of cyber intrusions into utilities, followed by extortion demands. We suspect, but cannot confirm, that some of these attackers had the benefit of inside knowledge. We have information that cyber attacks have been used to disrupt power equipment in several regions outside the United States. In at least one case, the disruption caused a power outage affecting multiple cities. We do not know who executed these attacks or why, but all involved intrusions through the Internet."

According to Mr. Donahue, the CIA actively and thoroughly considered the benefits and risks of making this information public, and came down on the side of disclosure.

August 2008 – Presidential Candidates Hacked

Possibly THE event that most likely shaped the President's resolve to create a cyber czar position.

President **Barack Obama** outlined his plan to better protect computer networks, including a new White House office headed by a cybersecurity czar. In the process, he disclosed he knows the risks firsthand.

“I know how it feels to have privacy violated because it has happened to me and the people around me,” he said at the morning event. “It’s no secret that my presidential campaign harnessed the Internet and technology to transform our politics. What isn’t widely known is that during the general election hackers managed to penetrate our computer systems.”

Obama called the incident “a powerful reminder: In this Information Age, one of your greatest strengths — in our case, our ability to communicate to a wide range of supporters through the Internet — could also be one of your greatest vulnerabilities.”

Not One, but BOTH Candidates...



WASHINGTON (CNN) -- Computers at the headquarters of the Barack Obama and John McCain campaigns were hacked during the campaign by a foreign entity looking for future policy information, a source with knowledge of the incidents confirms to CNN.

The source said the computers were hacked mid-summer by either a foreign government or organization.



April 2009 - Hackers Steal Information on Pentagon's Newest Fighter Jet (F-35)

WASHINGTON (CNN) -- Thousands of confidential files on the U.S. military's most technologically advanced fighter aircraft have been compromised by unknown computer hackers over the past two years, according to senior defense officials.

The Internet intruders were able to gain access to data related to the design and electronics systems of the Joint Strike Fighter through computers of Pentagon contractors in charge of designing and building the aircraft, according to the officials, who did not want to be identified because of the sensitivity of the issue.

In addition to files relating to the aircraft, hackers gained entry into the Air Force's air traffic control systems, according to the officials. Once they got in, the Internet hackers were able to see such information as the locations of U.S. military aircraft in flight.

April 2009

Hackers Embedded Code in the Power Grid

WASHINGTON (CNN) -- Computer hackers have embedded software in the United States' electricity grid and other infrastructure that could potentially disrupt service or damage equipment, two former federal officials told CNN.

The code in the power grid was discovered in 2006 or 2007, according to one of the officials, who called it "the 21st century version of Cold War spying."

Department of Homeland Security Director Janet Napolitano would not confirm such a breach, but said Wednesday that there has been no known damage caused by one.

The U.S. power grid isn't the only system at risk. The former officials said malicious code has been found in the computer systems of oil and gas distributors, telecommunications companies and financial services industries.

Supply Chain Risk Management

Fake Cisco Router Scam

Nearly all of the integrated circuit industry is controlled by foreign countries

Microsoft and other vendors established foreign partnerships for the design and development of software

ShenZhen, PRC



Scope of the Problem

- Alliance for Gray Market and Counterfeit Abatement (AGMA) & KPMG White Paper
 - 1 in 10 IT products sold are counterfeit
 - 10% IT products counterfeit
 - \$100 billion

Next... the Legal Landscape

Some Federal Cyber Statutes

Statutes fall into several broad categories:

Homeland – Statutes that govern homeland are often called Homeland Security Presidential Directives (HSPDs)

Intelligence Community – Statutes that govern the Intelligence Community are called Intelligence Community Directives (ICDs)

Law Enforcement (Federal) / Criminal – Statutes for law enforcement are largely federal statutes

Federal Domains

Law Enforcement (LE) : FBI, SS, IG

Department of Homeland Security (DHS) – Federal computer security

Office of Management and Budget (OMB) – Federal community best practices

White House (National Security Council, Homeland Security Council) – control the National Security Process

Applicable Laws

[HSPD – 5: Management of Domestic Incidents](#). Enhances the ability of the United States to manage domestic incidents by establishing a single, comprehensive national incident management system.

[HSPD – 7: Critical Infrastructure Identification, Prioritization, and Protection](#). Establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks.

[HSPD – 8: National Preparedness](#). Identifies steps for improved coordination in response to incidents. This directive describes the way Federal departments and agencies will prepare for such a response, including prevention activities during the early stages of a terrorism incident. This directive is a companion to HSPD-5.

[HSPD – 8 Annex 1: National Planning](#). Further enhances the preparedness of the United States by formally establishing a standard and comprehensive approach to national planning.

[HSPD – 12: Policy for a Common Identification Standard for Federal Employees and Contractors](#). Establishes a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees). [HSPD – 20: National Continuity Policy](#). Establishes a comprehensive national policy on the continuity of federal government structures and operations and a single National Continuity Coordinator responsible for coordinating the development and implementation of federal continuity policies.

[HSPD – 20 Annex A: Continuity Planning](#). Assigns executive departments and agencies to a category commensurate with their COOP/COG/ECG responsibilities during an emergency.

HSPD – 23/NSPD-54: Comprehensive National Cyber Security Initiative.

Authorities and Policies

- Homeland Security Presidential Directive-5 (HSPD-5)
- [?] Homeland Security Presidential Directive-7 (HSPD-7)
- [?] Federal Information Security Management Act (FISMA)
- [?] Executive Order 12472: The Assignment of National Security Emergency Preparedness
- Responsibilities for Telecommunications
- [?] Section 706, Communications Act of 1934, as amended (47 U.S.C. 606)
- [?] The Defense Production Act of 1950, as amended
- [?] National Security Act of 1947, as amended
- [?] National Security Directive 42: National Policy for the Security of National Security
- Telecommunications and Information Systems
- [?] Executive Order 12333: United States Intelligence Activities, as amended
- [?] National Strategy to Secure Cyberspace

More Authorities

- The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)

Information Sharing

- **Under IRTPA, the Information Sharing Environment was established and the Information Sharing Council (ISC) was created**
 - **Being moved under the Information Sharing and Access Policy Inter-agency Policy Committee (IPC)**

Information Sharing Public / Private Partnership

003469

THE WHITE HOUSE

WASHINGTON

July 2, 2009

SUBJECT: Strengthening Information Sharing and Access

Achieving effective information sharing and access throughout the government is a top priority of the Obama administration. This priority extends beyond terrorism-related issues, to the sharing of information more broadly to enhance the national security of the United States and the safety of the American people. Significant progress has been made in recent years. Concerted steps have been taken to facilitate information sharing and access across federal, state, local, tribal, and private sector communities, while protecting privacy and civil liberties. But there is more work to be done.

<http://www.fas.org/sgp/obama/brennan070209.pdf>

Information Sharing and Cyber

- **IRTPA established a Program Manager and Information Sharing Environment (PM-ISE)**
 - **ISE Serves Five Communities:**
 - **Law Enforcement, Homeland Security, Intelligence Community, Defense & Foreign Affairs**
 - **Integrating “cyber” into one of the above categories is not always intuitive**

Espionage Definitions Related to Cyber Crimes

- **Economic Espionage** is (1) whoever knowingly performs targeting or acquisition of trade secrets to (2) knowingly benefit any foreign government, foreign instrumentality, or foreign agent. (Title 18 U.S.C., Section 1831).
- **Industrial Espionage** is theft of trade secrets occurs when someone (1) knowingly performs targeting or acquisition of trade secrets or intends to convert a trade secret to (2) knowingly benefit anyone other than the owner. (Title 18 U.S.C., SECTION 1832).

Economic and Industrial Espionage

- According to the American Society for Industrial Security, economic and industrial espionage cost US businesses an estimated \$59 billion in 2005.
- The Economic Espionage Act of 1996 permits legal action regarding “financial, business, scientific, engineering, technical and economic information,” if a company can demonstrate it has attempted to keep this information classified and protected.
- Most information reported as having been compromised was physically located in the U.S. when the compromise occurred, but foreign entities were the major beneficiaries.
- Information assets in all formats (paper, electronic, oral, prototypes, and models) are being targeted for possible compromise.
- Information compromises have resulted in losses to reputation, image, goodwill, competitive advantage, core technology, and profitability.

More on Economic Espionage

February 8, 2008

Trojan Dragon: China's Cyber Threat

by [John J. Tkacik, Jr.](#)

Backgrounder #2106

America's counterintelligence czar, Dr. Joel F. Brenner, painted an alarming picture of economic espionage in 2006, albeit in the objective tones and neutral parlance of the intelligence community. He reported to Congress that "foreign collection efforts have hurt the United States in several ways": Foreign technology collection efforts have "eroded the US military advantage by enabling foreign militaries to acquire sophisticated capabilities that might otherwise have taken years to develop." "[M]assive" industrial espionage has "undercut the US economy by making it possible for foreign firms to gain a competitive economic edge over US companies." [\[1\]](#)

Ghostnet

10-month investigation of alleged Chinese cyber spying against Tibetan institutions.

The investigation ultimately uncovered a network of over 1,295 infected hosts in 103 countries.

Up to 30% of the infected hosts are considered high-value targets and include computers located

at ministries of foreign affairs, embassies, international organizations, news media, and NGOs. The Tibetan computer systems we manually investigated, and from which our investigations began, were conclusively compromised by multiple infections that gave attackers unprecedented access to potentially sensitive information.

Other Policy Drivers

- Reports:
 - The Center for Strategic and International Studies (CSIS) (www.csis.org/cyber)
 - U.S. China Economic and Security Review Commission (www.uscc.gov)
 - General Accounting Office reports (www.gao.gov)
- Senate and Congressional hearings and testimony
 - [Homeland.house.gov](http://homeland.house.gov) (homeland.house.gov)
 - [Homeland.senate.gov](http://homeland.senate.gov)
 - http://www.senate.gov/pagelayout/committees/d_three_sections_with_teasers/committees_home.htm

Influence of CSIS Commission

- The Center for Strategic and International Studies: Commission on Cyber Security for the 44th President Report

Three Major Findings:

- 1) Cyber is a major national security problem
- 2) Decisions and actions must respect privacy & civil liberties
- 3) Only a national cyber security policy that embraces both domestic and international aspects of cybersecurity will make us more secure.

CSIS Recommendations

- To the President:
 - Create a comprehensive national security strategy for cyberspace
 - Lead from the White House
 - Re-invent the public-private partnership
 - Regulate cyberspace
 - Authenticate digital identities
 - Modernize authorities
 - Use acquisitions policy to improve security
 - Build capabilities
 - Do not start over

CSIS - more

- Recommended the President create a Cybersecurity Directorate under the National Security Council (NSC)
 - National Office for Cyberspace (NOC)
 - Merge the DHS/National Cyber Security Center (NCSC) and the ODNI/Joint Inter-Agency Cyber Task Force (JIACTF)

DHS and the NOC

- Cyber is much like Weapons of Mass Destruction:
 - Diplomatic
 - International
 - Economic
- DHS has the authorities to be responsible for homeland security issues
- National Office for Cyberspace (NOC) would be responsible for the diplomatic, economic and International relations and policy related to these

Notable Quotes from the Noteworthy

- **Experts fear cyber-attack on U.S.
Government's response to threat is too little, too late, they say**
Author: JEFF NESMITH Cox News Service
Publish Date: December 20, 1998
- The government has responded to the threat of cyber-war with ideas and policies that are outdated before they can be implemented, a leading national security think tank warns.
- Many officials fail to appreciate the dangers of "weapons of mass disruption," said analysts from the Center for Strategic and International Studies.
- Terrorist organizations and doomsday sects with relatively little financing could use computers and widely available know-how to launch an attack that could cause financial devastation

How Does This Affect You?

- Personally
 - Cyber security professional licensing requirements?
 - Legislation affecting Personal liability?
- Organization
 - Regulation –
 - Mandatory security baseline standards for “Critical Infrastructure”
 - Required compliance for federal contracts
 - Mandatory incident reporting (centralized/consolidated)

Why Do You Care?

These policies and laws impact the federal government's relationship with State, local and tribal governments, and private industry

How - Information sharing – no common laws to govern the protection of sensitive information

Regulation is likely inevitable under current administration culture (and recent events)

What Can You Do?

- Reach out to your local FBI Infragard office (links provided in resources) and establish relationship BEFORE major event occurs
- Stay current on the policies – review and comment where possible



InfraGard®
a collaboration for
infrastructure protection



HOME

ABOUT INFRAGARD

BECOME A MEMBER

FIND YOUR CHAPTER

NEWS ROOM

LINKS

CONTACT

SPECIAL INTEREST GROUPS



18-Sep-2009

31,984 MEMBERS (Including FBI)

LEARN MORE ABOUT INFRAGARD®

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the [Federal Bureau of Investigation](#) and the private sector. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. [InfraGard Chapters](#) are geographically linked with FBI Field Office territories. [Learn more about InfraGard](#)

IN THE NEWS

📄 [Fordham Students Test Cyber Security Skills in War Games](#)

Computer and information science (CIS) students at Fordham honed their computer

 **ELEVATED**
significant risk of terrorist attacks

BECOME A MEMBER

APPLY FOR MEMBERSHIP

Attend a local chapter meeting, meet FBI officials from your area, and help protect your nation's infrastructure today. 📄

INFRASTRUCTURE PROTECTION

It is our goal to improve and extend information sharing between private industry and the government, particularly the FBI, when it comes to critical national infrastructures.

FEATURED CHAPTER
NATIONS CAPITAL

INFRAGARD
MEMBERS

Critical Infrastructures: Today

As defined by the President of the United States in 1998:

"Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. These systems are so vital, that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States."

Infrastructure Sectors:



Critical Infrastructure: Near Future

- Financial
- Telecommunications
- Energy
- Chemical, Nuclear, Biological (Chem Nuke Bio)

References, Links and Resources

<http://www.infragard.net/>

<http://infragardlosangeles.org/Infrastructure.html>

<http://csis.org/program/commission-cybersecurity-44th-presidency>

<http://www.opencongress.org>

<http://www.gcn.com/Articles/2006/08/17/Red-storm-rising.aspx>

<http://www.usdoj.gov/criminal/cybercrime/>

http://www.markle.org/downloadable_assets/20090730_jsmith_testimony.pdf

