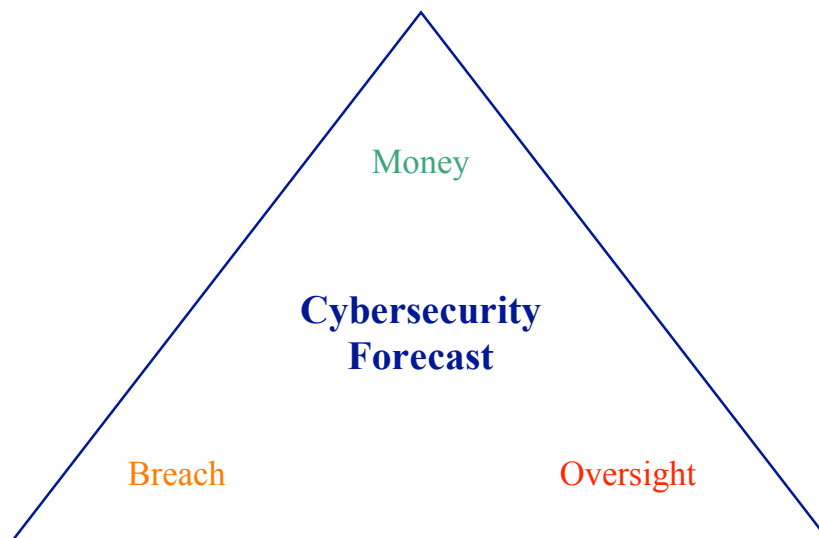




**The Cyber Forecast -- Hotter Than Global Warming:  
A Review of 2007 and Preview of 2008 in Cybersecurity**

by

**David Z. Bodenheimer**



**The DC Cyber Security  
Breakfast Series**

*Cyberspace & Homeland Security  
Vulnerability & Opportunity*

January 24, 2008

**Crowell & Moring LLP**  
[www.crowell.com](http://www.crowell.com)  
1001 Pennsylvania Ave., NW  
Washington, DC 20004-2595  
(202) 624-2713  
[dbodenheimer@crowell.com](mailto:dbodenheimer@crowell.com)

## **The Cyber Forecast -- Hotter Than Global Warming: A Review of 2007 and Preview of 2008 in Cyber Security**

In the cyber realm, momentum is building – and the primary drivers are hemorrhaging security breaches, sizzling oversight, and mushrooming money. In fact, the relationship is virtually mathematical:

Security Breaches → Oversight → Money

In the past five years, cybersecurity has shifted from an IT insider's worry to a popular media and political obsession. One way to track this trajectory at a glance is through the headlines:

### **2005: The Year of Personal Information Insecurity**

“Hackers Tap 40 Million Credit Cards,” *Los Angeles Times*  
(June 18, 2005)

“Burned by ChoicePoint Breach, Potential ID Theft Victims Face a Lifetime of Vigilance,” *Information Week* (Feb. 24, 2005)

“2005 Worst Year for Breaches of Computer Security,” *USA Today* (Dec. 29, 2005)

### **2006: The Year of Federal Information Insecurity**

“Vast Data Cache About Veterans Is Stolen,” *New York Times*  
(May 23, 2006)

“FTC Reports Laptop is Stolen in Latest U.S. Data Breach,” *Wall Street Journal* (June 23, 2006)

“Navy Probes Data Leak on 100,000 Sailors, Marines,” *Reuters*  
(July 7, 2006)

### **2007: The Year of Oversight for Information Insecurity**

“Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure,” Statement of Rep. Thompson (Apr. 19, 2007)

“Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses,” GAO (July 27, 2007)

“Challenges Remain in Securing the Nation's Cyber Infrastructure,”  
DHS Inspector General (June 2007)

## **I. Security Breach Forecast: Blizzard Conditions Will Worsen**

By any measure, security breach has become everyone's problem. For 2007, a blizzard of new security breaches have set new records for compromised personal information.

### **A. Security Breach & Cybercrime by the Numbers**

Since 2005, security breaches have skyrocketed, exposing personal information in both government and private hands. Even at a glance, the numbers are sobering.

- Sensitive Personal Information Records Breached
  - **127 million** records compromised in 2007<sup>1</sup>
  - **600% increase** over 2006<sup>2</sup>
  - **217 million** records breached since 2005<sup>3</sup>
- Cybercrime Costs
  - **\$105 billion** worldwide in 2007<sup>4</sup>
  - Outstripped illegal drug trafficking
- US CERT Data
  - **37,000 incidents** (Oct. 2006 to Sept. 2007)<sup>5</sup>
  - **24,000 incidents** (Oct. 2005 to Sept. 2006)
  - **54% increase** (over 1-year period)

---

<sup>1</sup> "2007 Data Breach Stats," Identity Theft Resources Center (ITRC)  
<http://idtheftmostwanted.org/ITRC%20Breach%20Stats%20Report%202007.pdf>

<sup>2</sup> "2006 Disclosures of U.S. Data Incidents," ITRC (over 19 million potentially affected in 2006)  
<http://idtheftmostwanted.org/ITRC%20Breach%20Report%202006.pdf>

<sup>3</sup> "Chronology of Data Breaches," Privacy Rights Clearinghouse (updated Jan. 20, 2008)  
<http://www.privacyrights.org/ar/ChronDataBreaches.htm#CP>

<sup>4</sup> O'Connell, "Cyber-Crime Hits \$100 Billion in 2007, Outearning Illegal Drug Trade," *Internet Business Law Services* (Oct. 15, 2007)

<sup>5</sup> "Remarks of Assistant Secretary of Cybersecurity & Communications, Greg Garcia at the New York Metro Infragard Alliance Security Summit," DHS Release (Dec. 11, 2007)  
[http://www.dhs.gov/xnews/releases/pr\\_1197409593155.shtm](http://www.dhs.gov/xnews/releases/pr_1197409593155.shtm)

## B. Private Sector Breaches & Vulnerabilities

- TJX Security Breach
  - **46 to 94 million** records exposed<sup>6</sup>
  - **\$40.9 million** likely settlement with credit card company<sup>7</sup>
  - **\$12 million** earnings hit (1<sup>st</sup> Quarter 2007)<sup>8</sup>
- Breaches & Vulnerabilities
  - **85% data breaches** (midsize & large businesses)<sup>9</sup>
    - 59% faced potential litigation
    - 32% experienced decline in share prices
  - **21% of attacks cost over \$100,000** (11% over \$500,000)<sup>10</sup>

## C. Federal Agency Security Breaches -- 2007

“TSA Laptops with Personal Info Missing,” *Associated Press* (Oct. 15, 2007)

- 3,930 commercial HAZMAT drivers

“Whacking Hackers,” *Newsweek* (Oct. 15, 2007)

- 1,500 Pentagon computers hacked, disabled

“Contractor Blamed in DHS Data Breaches,” *Washington Post* (Sept. 24, 2007)

- FBI investigation of Chinese hacker break-in

“Monster Theft Also Hit Government Site,” *USA Today* (Aug. 31, 2007)

- 146,000 users’ contact information stolen from USAjobs.gov

“Lax and Lazy at Los Alamos,” *Newsweek* (June 25, 2007)

- Leak of highly classified data from nuclear lab

---

<sup>6</sup> “2007 Was Year of Data Breach,” States News Service (Jan. 1, 2008).

<sup>7</sup> Jewell, “TJX to Pay Up to \$41M over Data Breach,” *Worcester Telegram & Gazette* (Dec. 1, 2007).

<sup>8</sup> “Asking for Trouble: Most Companies Don’t Have Plans to Handle Data Breach,” CMP TechWeb (May 22, 2007).

<sup>9</sup> *Id.*, citing Ponemon Institute survey.

<sup>10</sup> “National Survey Finds Organizations Continue to Experience High Rate of Cyber Attacks,” *Business Wire* (Jan. 30, 2006).

## II. Cyber Oversight: Hail and Lightning Are Striking Hard

In the information security business, oversight comes from all directions – Congress, GAO, Inspectors General, OMB, the courts – and more.

### A. Congressional Oversight

Congress – particularly the House Homeland Security Committee – has been particularly active in exercising oversight through hearings, reports, and investigations of information security shortfalls and gaps for both federal agencies and the private sector.

“Information Security Breach at TSA: The Traveler Redress Website,” Report of House Oversight and Government Reform Majority Staff (Jan. 2008)  
<http://www.hsc.house.gov/hearings/index.asp?ID=36>

“Enhancing and Implementing the Cybersecurity Elements of the Sector Specific Plans,” Hearings before House Homeland Security Subcommittees (Oct. 31, 2007) <http://www.hsc.house.gov/hearings/index.asp?ID=100>

“Thompson Demands Details on Administration’s Cyber Initiative,” House Homeland Security News Alert (Oct. 24, 2007)  
<http://www.hsc.house.gov/press/index.asp?ID=288&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

“Langevin, McCaul, Jackson-Lee Inquire on Electrical Grid Security,” House Homeland Security News Alert (Oct. 19, 2007)  
<http://www.hsc.house.gov/press/index.asp?ID=283&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

“The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid,” Hearings before House Homeland Security Subcommittee (Oct. 17, 2007)  
<http://www.hsc.house.gov/hearings/index.asp?ID=95>

“Thompson, Langevin Demand Investigation into Department Cyber Attacks,” House Homeland Security Committee News Alert (Sept. 24, 2007)  
<http://www.hsc.house.gov/press/index.asp?ID=268&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

“Thompson, Langevin Inquire on DHS Cybersecurity,” House Homeland Security Committee News Alert (July 27, 2007)  
<http://www.hsc.house.gov/press/index.asp?ID=255&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

“Lieberman Calls on Federal Agencies to Safeguard Information Networks,” Senate Homeland Security & Governmental Affairs Committee Press Release (July 27, 2007)

[http://hsgac.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease\\_id=1521&Affiliation=C](http://hsgac.senate.gov/index.cfm?FuseAction=PressReleases.Detail&PressRelease_id=1521&Affiliation=C)

“Thompson, Langevin Release GAO Cybercrime Report, Announce Plans to Improve Private Sector Cybersecurity,” House Homeland Security Committee News Alert (July 23, 2007)

<http://www.hsc.house.gov/press/index.asp?ID=251&SubSection=2&Issue=0&DocumentType=0&PublishDate=0>

“Hacking the Homeland: Investigating Vulnerabilities at the Department of Homeland Security,” Hearings before House Homeland Security Committee (June 20, 2007) <http://www.hsc.house.gov/hearings/index.asp?ID=65>

“Thompson, Langevin Inquire on Cybersecurity at Nuclear Plants,” House Homeland Security Committee News Alert (May 18, 2007)

<http://www.hsc.house.gov/press/index.asp?ID=212&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

“Addressing the Nation’s Cybersecurity Challenges: Reducing Vulnerabilities Requires Strategic Investment and Immediate Action,” Hearings Before House Homeland Security Subcommittee (Apr. 24, 2007)

<http://www.hsc.house.gov/hearings/index.asp?ID=41>

“Cyber Insecurity: Hackers are Penetrating Federal Systems and Critical Infrastructure,” Hearings before House Homeland Security Subcommittee (Apr. 18, 2007) <http://www.hsc.house.gov/hearings/index.asp?ID=36>

## **B. Government Accountability Office (GAO) Reports**

In 2007 and 2008, GAO’s information security reviews cut across nearly every federal agency and identified pervasive weaknesses in protection of highly-sensitive – and in some cases, classified – data.

“Information Security: IRS Needs to Address Pervasive Weaknesses,” GAO (GAO-08-211) (Jan. 2008)

<http://www.gao.gov/new.items/d08211.pdf>

“Veterans Affairs: Sustained Management Commitment and Oversight Are Essential to Completing Information Technology Realignment and Strengthening Information Security,” GAO (GAO-07-1264T) (Sept. 2007)

<http://www.gao.gov/new.items/d071264t.pdf>

“Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain,” GAO (GAO-07-1036) (Sept. 2007)

<http://www.gao.gov/new.items/d071036.pdf>

“Information Security: Sustained Management Commitment and Oversight are Vital to Resolving Long-Standing Weaknesses at the Department of Veterans Affairs, GAO (GAO-07-1019)  
<http://www.gao.gov/new.items/d071019.pdf>

“Information Security: Selected Departments Need to Address Challenges in Implementing Statutory Requirements,” GAO (GAO-07-528) (Aug. 31, 2007)  
<http://www.gao.gov/new.items/d07528.pdf>

“Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses,” GAO (GAO-07-837) (July 27, 2007)  
<http://www.gao.gov/new.items/d07837.pdf>

“Information Security: Homeland Security Needs to Immediately Address Significant Weaknesses in Systems Supporting the US-VISIT Program,” GAO (GAO-07-870) (July 13, 2007)  
<http://www.gao.gov/new.items/d07870.pdf>

“Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats,” GAO (GAO-07-705) (June 22, 2007)  
<http://www.gao.gov/new.items/d07705.pdf>

“Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program,” GAO (GAO-07-1003T) (June 20, 2007)  
<http://www.gao.gov/new.items/d071003t.pdf>

“Bureau of the Public Debt: Areas for Improvement in Information Security Controls,” GAO (GAO-07-899R) (June 14, 2007)  
<http://www.gao.gov/new.items/d07899r.pdf>

“Information Security: Agencies Report Progress, but Sensitive Data Remain at Risk,” GAO (GAO-07-935T) (June 7, 2007)  
<http://www.gao.gov/new.items/d07935t.pdf>

“Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown,” GAO (GAO-07-737) (June 4, 2007)  
<http://www.gao.gov/new.items/d07737.pdf>

“Information Security: Federal Deposit Insurance Corporation Needs to Sustain Progress Improving Its Program,” GAO (GAO-07-351) (May 18, 2007)  
<http://www.gao.gov/new.items/d07351.pdf>

“Information Security: FBI Needs to Address Weaknesses in Critical Network,” GAO (GAO-07-368) (Apr. 30, 2007)  
<http://www.gao.gov/new.items/d07368.pdf>

“Privacy: Lessons Learned about Data Breach Notification,” GAO (GAO-07-657) (Apr. 30, 2007)  
<http://www.gao.gov/new.items/d07657.pdf>

“Information Security: Persistent Weaknesses Highlight Need for Further Improvement,” GAO (GAO-07-751T) (Apr. 19, 2007)  
<http://www.gao.gov/new.items/d07751t.pdf>

“Information Security: Sustained Progress Needed to Strengthen Controls at the Securities and Exchange Commission,” GAO (GAO-07-256) (Mar. 27, 2007)  
<http://www.gao.gov/new.items/d07256.pdf>

“Information Security: Veterans Affairs Needs to Address Long-Standing Weaknesses,” GAO (GAO-07-732T) (Feb. 28, 2007)  
<http://www.gao.gov/new.items/d07532t.pdf>

### **C. Inspector General (IG) Reports**

The Offices of Inspector General for numerous agencies issued a host of reports in 2007 and 2008 criticizing information security. Examples from DHS and DOE include:

“Incident of Security Concern at the Y-12 National Security Complex,” DOE OIG (DOE/IG-0785) (Jan. 2008)  
<http://ig.energy.gov/documents/IG-0785.pdf>

“Information Technology Management Needs to Be Strengthened at the Transportation Security Administration,” DHS OIG (OIG-08-07) (Oct. 2007)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_08-07\\_Oct07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_08-07_Oct07.pdf)

“Better Administration of Automated Targeting System Controls Can Further Protect Personally Identifiable Information,” DHS OIG (OIG-08-06) (Oct. 2007)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_08-06\\_Oct07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_08-06_Oct07.pdf)

“Progress Has Been Made But More Work Remains in Meeting Homeland Security Presidential Directive 12 Requirements,” DHS OIG (OIG-08-01) (Oct. 2007)  
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_08-01\\_Oct07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_08-01_Oct07.pdf)

“Evaluation of DHS’ Information Security Program for Fiscal Year 2007,” DHS OIG (OIG-07-77) (Sept. 2007)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_07-77\\_Sep07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_07-77_Sep07.pdf)

“Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security (Redacted),” DHS OIG (OIG-07-50) (June 2007)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_07-77\\_Sep07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_07-77_Sep07.pdf)

“Challenges Remain in Securing the Nation’s Cyber Infrastructure,” DHS OIG (OIG-07-48) (June 2007)

[http://www.dhs.gov/xoig/assets/mgmttrpts/OIG\\_07-48\\_Jun07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIG_07-48_Jun07.pdf)

“DHS’s Implementation of Protective Measures for Personally Identifiable Information,” DHS OIG (OIG-07-24) (Jan. 2007)

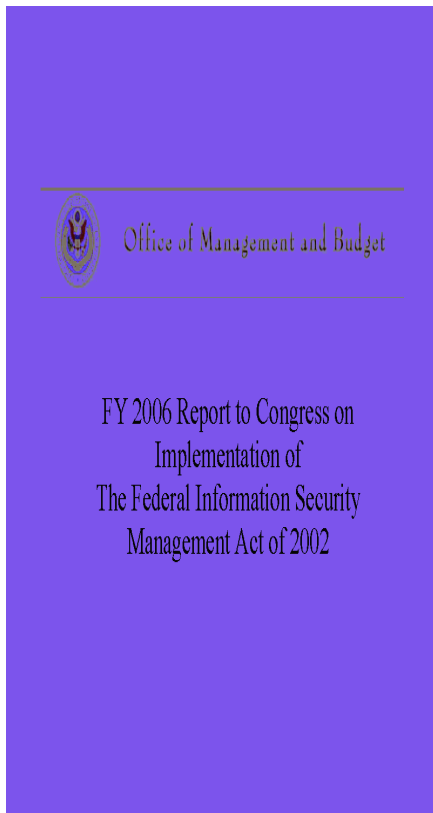
[http://www.dhs.gov/xoig/assets/mgmttrpts/OIGr\\_07-24\\_Jan07.pdf](http://www.dhs.gov/xoig/assets/mgmttrpts/OIGr_07-24_Jan07.pdf)

#### D. Office of Management & Budget (OMB) Oversight

Under FISMA, OMB has a statutory responsibility to oversee information security for federal agencies. 44 U.S.C. §§ 3541-49. In the most recent report to Congress, OMB said federal agencies have made progress. But the grades are still not very good.

**Table 3. Quality of Certification and Accreditation Processes**  
OMB is responsible for overseeing the effectiveness of agency security procedures. Agency IGs were asked to evaluate the quality of agency certification and accreditation processes. They were given response choices including: excellent, good, satisfactory, poor and failing.

Agency	Evaluation
Agency for International Development	Good
Department of Agriculture	Poor
Department of Commerce	Poor
Department of Defense	Poor
Department of Education	Satisfactory
Department of Energy	Poor
Environmental Protection Agency	Satisfactory
General Services Administration	Satisfactory
Department of Health and Human Services	Good
Department of Homeland Security	Satisfactory
Department of Housing and Urban Development	Satisfactory
Department of the Interior	Poor
Department of Justice	Good
Department of Labor	Good
National Aeronautics and Space Administration	Poor
National Science Foundation	Good
Nuclear Regulatory Commission	Failing
Office of Personnel Management	Excellent
Small Business Administration	Satisfactory
Smithsonian Institution	Satisfactory
Social Security Administration	Excellent
Department of State	Satisfactory
Department of Transportation	Good
Department of the Treasury	Poor
Department of Veterans Affairs	Poor
Total “Excellent”:	2
Total “Good”:	6
Total “Satisfactory”:	8
Total “Poor”:	8
Total “Failing”:	1



[http://www.whitehouse.gov/omb/inforeg/reports/2006\\_fisma\\_report.pdf](http://www.whitehouse.gov/omb/inforeg/reports/2006_fisma_report.pdf)

## E. Litigation Oversight

Litigation follows money – and security breaches. As a result, companies in the cybersecurity business will increasingly see litigation swirling around all things cyber.

### 1. Potential Criminal Investigation & Prosecution

For both federal agencies and contractors, the stakes are increasing as failed cybersecurity may lead to criminal investigations and potential prosecution.

BENNE G. THOMPSON, MISSISSIPPI  
CHAIRMAN



PETER T. KING, NEW YORK  
RANKING MEMBER

One Hundred Tenth Congress  
U.S. House of Representatives  
Committee on Homeland Security  
Washington, DC 20515

September 21, 2007

Richard L. Skinner  
Inspector General  
Department of Homeland Security  
Washington, D.C. 20528

Dear Inspector General Skinner:

Over the previous five months, the House Committee on Homeland Security has investigated the information technology security posture at the Department of Homeland Security. The results of our investigation suggest that the Department is the victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks. We ask you to immediately commence an inquiry into these matters, and, if necessary, refer this matter for criminal investigation.

**Thompson, Langevin  
Demand Investigation  
into Department  
Cyber Attacks  
(Sept. 24, 2007)**

Where DHS and its contractor did not take certain information security precautions, hackers penetrated the system, compromising dozens of computers and exfiltrating information to services connecting to Chinese websites.

<http://www.hsc.house.gov/press/index.asp?ID=268&SubSection=0&Issue=0&DocumentType=0&PublishDate=0>

### 2. Protest Litigation

As more federal money flows into cybersecurity, competing contractors will become increasingly willing to protest awards involving information security technology. For example, GAO recently sustained a protest involving a Department of Justice (DOJ) solicitation for services to support information security programs. *See Superlative Technologies, Inc.*, B-310489 *et al.*, Jan. 4, 2008 (<http://www.gao.gov/decisions/bidpro/310489.pdf>)

### 3. Security Breach Litigation

Class-action lawsuits have been a common response to a security breach. For example, the American Federation of Government Employees (AFGE) filed a class action in the U.S. District Court in the District of Columbia against TSA for loss or theft of 100,000 payroll records of current and former employees. In the suit, the labor union alleged violations of the

security and confidentiality requirements under the Privacy Act, as well as the Aviation and Transportation Security Act.<sup>11</sup> As Senator Lieberman pointed out, “TSA has compromised the information of airport security officers, air marshals and other TSA law enforcement officers.”

### **III. Money for Cybersecurity: After a Drought Comes the Monsoon**

For years, independent commissions, security experts and others have called for more money for cybersecurity. For years, cybersecurity funding has remained relatively flat. However, 2008 and 2009 will see a substantial funding ramp-up for a number of reasons.

#### **A. Critical Infrastructure Protection**

Much of the burden for security falls upon the private sector which “controls 85 percent of the critical infrastructure in the nation.” National Commission on Terrorist Attacks upon the United States, *The 9/11 Commission Report*, p. 398. Several statutory and regulatory developments will increase the impetus for private sector effort to bolster information security.

##### **1. Chemical Cybersecurity**

The Fiscal Year 2007 Homeland Security Appropriations Act imposed additional security requirements upon chemical facilities. Pub. L. No. 109-295, § 550. In the implementing regulations, DHS expressly required chemical facilities to address cybersecurity in their Site Security Plans:

The Department recognizes that cyber security is an issue and has included cyber security as one of the performance standards that facilities must address in their Site Security Plan. Paragraph (c)(8) requires facilities to select, develop, and implement measures that “deter cyber sabotage.” In addition, the Department notes that it has implemented an assessment of cyber vulnerabilities for industrial control systems within the CSAT Security Vulnerability Assessment.

72 Fed. Reg. 17706 (2007); 6 C.F.R. § 27.230(c)(8) (2007). With the issuance of Appendix A in November 2007 (72 Fed. Reg. 65396), chemical facilities will be preparing vulnerability assessments and security plans that will include steps to address cybersecurity.

##### **2. Surface Transportation Cybersecurity**

In the 9/11 legislation, Congress required certain rail and bus carriers to perform “vulnerability assessments and security plans” addressing the security of “information systems,” including “programmable electronic devices, computers or other automated systems” which are used in such transportation. Pub. L. No. 110-53, §§ 1512(d)(1) (railroad carriers) and 1531(d)(1) (bus carriers). In addition, the 9/11 Act authorizes \$25 million per year (FY 2008-11) for “public

---

<sup>11</sup> Mosquera, “Union Files Suit Against TSA for Data Breach,” *Federal Computer Week* (May 9, 2007).

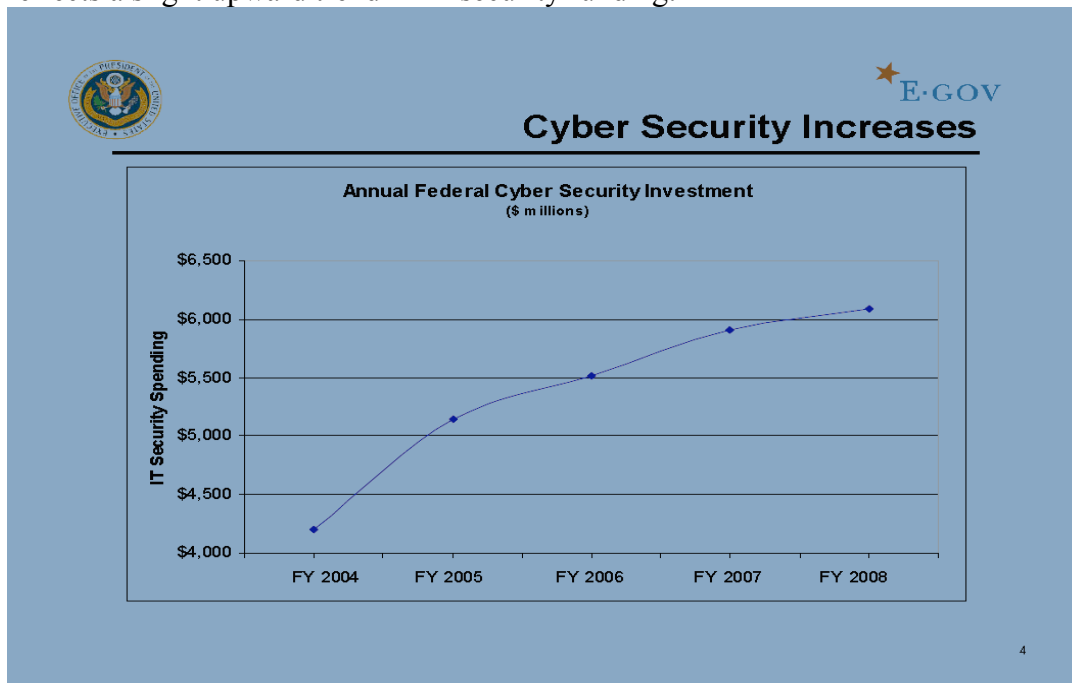
transportation research and development” grants that may be used for such purposes as “research technologies that mitigate damages in the event of a cyber attack.” Pub. L. No. 110-53, § 1409(c)(2)(F).

### 3. Power Grid Cybersecurity

As part of the Energy Policy Act of 2005 (Pub. L. No. 109-58), Congress included the Electricity Modernization Act (Title XII) establishing mandatory reliability standards governing the electric power industry. These reliability standards include “cybersecurity protection” to ensure reliable operation “so that instability, uncontrolled separation, or cascading failure of such a system will not occur as a result of a sudden disturbance, including a cybersecurity incident, or an unanticipated failure of system elements.” Pub. L. No. 109-58, § 1211, 119 Stat. 941-42 (2005). Divided responsibility between DHS and FERC has slowed implementation. However, Congressional oversight – including hearings in 2007 – should speed up such efforts within the federal agencies and the power industry. “The Cyber Threat to Control Systems: Stronger Regulations are Necessary to Secure the Electric Grid,” Hearings before House Homeland Security Subcommittee (Oct. 17, 2007) <http://www.hsc.house.gov/hearings/index.asp?ID=95>; “Langevin, McCaul, Jackson-Lee Inquire on Electrical Grid Security,” House Homeland Security News Alert (Oct. 19, 2007).

#### B. IT Security Spending

For Fiscal Year (FY) 2008, the budget request seeks \$66.4 billion for information technology, with IT security accounting for 9.2% – \$6.092 billion – of this amount. This request reflects a slight upward trend in IT security funding:



OMB, “Fiscal Year 2008 Information Technology Budget (updated May 24, 2007), p. 4 [http://www.whitehouse.gov/omb/egov/documents/FY08\\_IT\\_Budget\\_Rollout\\_MayUpdate.pdf](http://www.whitehouse.gov/omb/egov/documents/FY08_IT_Budget_Rollout_MayUpdate.pdf).

## C. Cyber Priorities for 2008

For 2008, cybersecurity takes a front seat, with the President, DHS, and the Intelligence community all placing heightened emphasis on greater protection.

### 1. Additional Cyber Funding for FY 2008

In November 2007, President Bush asked for additional FY 2008 funds to be allocated to cybersecurity.<sup>12</sup>

THE WHITE HOUSE  
WASHINGTON

November 6, 2007

Dear Madam Speaker:

I ask the Congress to consider the enclosed amendments to my FY 2008 requests for the Departments of Homeland Security and Justice. These amendments, when combined with funding enacted earlier this year for the FBI (Public Law 110-28), would provide \$436 million to take important steps to enhance ongoing efforts for protecting the homeland. The amendments will enhance the security of the Government's civilian cyber networks and will further address emerging threats.

Overall, the discretionary budget authority proposed in my FY 2008 Budget would not be increased. The details of these amendments proposal are set forth in the enclosed letter from the Director of the Office of Management and Budget.

Sincerely,



According to OMB's budget breakdown, this FY 2008 amended request includes the following specific cyber efforts:

- “\$39 million to assist FBI’s investigations of incursions into the Government’s cyber networks, increase relevant intelligence analysis, and provide the necessary technical tools that support both investigations and analysis”;

---

<sup>12</sup> President Bush’s letter to Speaker Pelosi (Nov. 6, 2007) and supporting OMB rationale ([http://www.whitehouse.gov/omb/budget/amendments/amendment\\_11\\_6\\_07.pdf](http://www.whitehouse.gov/omb/budget/amendments/amendment_11_6_07.pdf)).

- “\$115 million for cybersecurity initiatives to enhance Federal civilian detection capabilities, including accelerated deployment of monitoring capabilities and increased analytical operations at United States Computer Emergency Readiness Team (US-CERT) to support civilian agencies.”

## 2. Top Homeland Security Priority

In December 2007, DHS Secretary Chertoff identified cybersecurity as one of his top four priorities for 2008.<sup>13</sup> As part of this effort, he specifically identified initiatives for expanding the Einstein Program (for detecting malicious patterns in computer network traffic) and “working with Congress, as we speak, on an enhanced cybersecurity strategy, which I believe will set the template for the next decade on how we deal with this emerging and increasing threat.”

## 3. Intelligence Priority

Since his “info-sec epiphany” at NSA, Admiral Mike McConnell (Director of National Intelligence) has been a strong proponent of both cyber warfare and defense.<sup>14</sup> During a meeting with President Bush in May 2007, Admiral McConnell warned that “[i]f the 9/11 perpetrators had focused on a single U.S. bank through cyber-attack and it had been successful, it would have an order-of-magnitude greater impact on the U.S. economy.” During that meeting, President Bush “charged McConnell to come up with a security strategy, not only for government systems but also for American industry and private individuals.” Based upon public sources, DNI’s “Cyber-Security Policy” remains in draft.<sup>15</sup> To implement the President’s direction and DNI’s cyber policy, substantial additional commitments of resources and funding are inevitable, as Admiral McConnell seeks to make his mark on information security in his remaining year at DNI.

DCIWDMs: 4883621\_1

---

<sup>13</sup> “Remarks by Homeland Security Secretary Michael Chertoff on 2007 Achievements and 2008 Priorities,” DHS New Release (Dec. 12, 2007) ([http://www.dhs.gov/xnews/speeches/sp\\_1197513975365.shtm](http://www.dhs.gov/xnews/speeches/sp_1197513975365.shtm)); Bain, “DHS Puts Cybersecurity Toward Top of 2008 To-Do List,” *Federal Computer Week* (Dec. 13, 2007).

<sup>14</sup> Wright, “The Spymaster: Can Mike McConnell fix America’s Intelligence Community,” *The New Yorker*, p. 51 (Jan. 21, 2008) (“Information security became McConnell’s passion”).

<sup>15</sup> *Id.*