AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

FEDERAL IT SECURITY: A REVIEW OF H.R. 4791

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

AND THE

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

SECOND SESSION

ON

H.R. 4791

TO AMEND TITLE 44, UNITED STATES CODE, TO STRENGTHEN REQUIREMENTS FOR ENSURING THE EFFECTIVENESS OF INFORMATION SECURITY CONTROLS OVER INFORMATION RESOURCES THAT SUPPORT FEDERAL OPERATIONS AND ASSETS, AND FOR OTHER PURPOSES

FEBRUARY 14, 2008

Serial No. 110–72

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

44–178 PDF WASHINGTON : 2008

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho
JIM JORDAN, Ohio

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT

EDOLPHUS TOWNS, New York, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CHRISTOPHER S. MURPHY, Connecticut
PETER WELCH, Vermont
CAROLYN B. MALONEY, New York

BRIAN P. BILBRAY, California
TODD RUSSELL PLATTS, Pennsylvania,
JOHN J. DUNCAN, Jr., Tennessee

MICHAEL McCARTHY, *Staff Director*

CONTENTS

	Page
Hearing held on February 14, 2008	1
Text of H.R. 4791	5
Statement of:	
Evans, Karen S., Administrator for Electronic Government and Information Technology, Office of Management and Budget; Gregory C. Wilshusen, Director, Information Security Issues, Government Accountability Office; Alan Paller, director of research, the Sans Institute; Bruce W. McConnell, president, McConnell International, LLC; and Tim Bennett, president, Cyber Security Industry Alliance	23
Bennett, Tim	93
Evans, Karen S.	23
McConnell, Bruce W.	82
Paller, Alan	65
Wilshusen, Gregory C.	33
Letters, statements, etc., submitted for the record by:	
Bennett, Tim, president, Cyber Security Industry Alliance, prepared statement of	96
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	3
Davis, Hon. Tom, a Representative in Congress from the State of Virginia:	
Letter dated July 27, 2007	104
Prepared statement of	108
Evans, Karen S., Administrator for Electronic Government and Information Technology, Office of Management and Budget, prepared statement of	26
McConnell, Bruce W., president, McConnell International, LLC, prepared statement of	84
Paller, Alan, director of research, the Sans Institute, prepared statement of	67
Wilshusen, Gregory C., Director, Information Security Issues, Government Accountability Office, prepared statement of	35

FEDERAL IT SECURITY: A REVIEW OF H.R. 4791

THURSDAY, FEBRUARY 14, 2008

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES, JOINT WITH THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,

Washington, DC.

The subcommittees met, pursuant to notice, at 11:30 a.m., in room 2154, Rayburn House Office Building, Hon. Wm. Lacy Clay (chairman of the Subcommittee on Information Policy, Census, and National Archives) presiding.

Present: Representatives Clay, Davis of Virginia, and Platts.

Staff present from the Information Policy, Census, and National Archives Subcommittee: Darryl Piggee, staff director/counsel; Jean Gosa, clerk; and Adam Bordes, professional staff member.

Staff present from the Government Management, Organization, and Procurement Subcommittee: Mike McCarthy, staff director; Velvet Johnson, counsel; Bill Jusino, professional staff member; and Kwane Drabo, clerk.

Mr. CLAY. Good morning. This hearing of the Oversight and Government Reform Committee is being held this morning by the Information Policy, Census, and National Archives Subcommittee, which I chair, and the Subcommittee on Government Management, Organization, and Procurement, chaired by Congressman Ed Towns of New York, who is under the weather this week and is not in town. But we will proceed without Mr. Towns.

This hearing will now come to order. Today's hearing will examine the important topic of Federal information security. Our subcommittees are holding this hearing because security is both a management and technology challenge.

Without objection, the Chair and ranking minority member will have 5 minutes to make opening statements, followed by opening statements not to exceed 3 minutes by other Members who wish to seek recognition.

Without objection, Members and witnesses may have 5 legislative days to submit a written statement or extraneous materials for the record.

Briefly, I would like to discuss some of the challenges that I see, and then I will yield to anyone else that shows up for comments.

Let me say that today's joint subcommittee hearing on the Current State of Federal Information Security and Legislation to Strengthen the Federal Information Security Management Act, I

am especially pleased to be teaming up with the Subcommittee on Government Management, Organization, and Procurement, chaired by Mr. Towns, for this critical issue.

For fiscal year 2009, the President's budget proposes spending of roughly $70 billion on information technology products alone. Yet according to OMB's 2006 FISMA report to Congress, agency efforts to implement effective information security programs are inconsistent throughout Government. These problems go beyond isolated data breaches and have exposed systemic information security vulnerabilities that have gone unmitigated by our agencies and the IT contracting community that serves them.

Having experienced 5 years of detailed OMB reporting through the FISMA process, I am certain that some real progress has been made in securing our agencies' IT assets. What I am unsure of, however, is whether our current requirements and OMB policies under FISMA are providing us enough tools to effective identify the inherent vulnerabilities in our systems, now or in the future.

With this in mind, I, along with Chairman Towns and Chairman Waxman, have put forward a bill that would move us toward more rigid security requirements for agency systems while staying with in the current FISMA framework. Furthermore, our bill will add consistency and robustness to the current program performance evaluation process by requiring an annual audit of agency programs. Last, this legislation begins to recognize the duty of care responsibilities that must be shared between both Federal agencies and the contracts providing services to them.

As technology evolves and the perimeters of IT enterprises expand, we must have a flexible security framework to harness such advances while ensuring that our networks remain secure. I am hopeful that our witnesses today will be ale to address these issues through the context of their experiences, and I look forward to their testimony.

[The prepared statement of Hon. Wm. Lacy Clay and the text of H.R. 4791 follow:]

Opening Statement
Wm. Lacy Clay (D-MO), Chairman
Information Policy, Census, and National Archives Subcommittee
House Committee on Oversight and Government Reform

Joint Hearing on "Federal IT Security: A Review of H.R. 4791"
before the Information Policy, Census, and National Archives Subcommittee and the
Subcommittee Government Management, Organization, and Procurement

Thursday, February 14, 2008
2154 Rayburn HOB
11:30 a.m.

Good morning and welcome to today's joint subcommittee hearing on the current state of federal information security, and legislation to strengthen the Federal Information Security Management Act. I am especially pleased to be teaming up with Chairman Towns of the Government Management Subcommittee in order to examine the critical issues involved with maintaining secure IT networks throughout our federal enterprise.

For FY 2009, the President's budget proposes spending roughly $70 billion on information technology products alone. Yet, according to OMB's 2006 FISMA (pronounced FIZZ-ma) Report to Congress, agency efforts to implement effective information security programs are inconsistent throughout the government. These problems go beyond isolated data breaches, and have exposed systemic information security vulnerabilities that have gone unmitigated by our agencies and the IT contracting community that serves them.

Having experienced five years of detailed OMB reporting through the FISMA process, I am certain that some

real progress has been made in securing our agencies IT assets. What I am unsure of, however, is whether our current requirements and OMB policies under FISMA are providing us enough tools to effectively identify the inherent vulnerabilities in our systems now or in the future.

With this in mind, I, along with my esteemed colleagues Mr. Towns and Chairman Waxman, have put forward a bill that would move us towards more rigid security requirements for agency systems while staying within the current FISMA framework. Furthermore, our bill will add consistency and robustness to the current program performance evaluation process by requiring an annual audit of agency programs. Lastly, this legislation begins to recognize the duty of care responsibilities that must be shared between both federal agencies and the contractors providing services to them.

As technology evolves and the perimeters of IT enterprises expand, we must have a flexible security framework to harness such advances while ensuring that our networks remain secure. I am hopeful that our witnesses today will be able to address these issues through the context of their experiences, and I look forward to their testimony.

I

110TH CONGRESS
1ST SESSION

H. R. 4791

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

DECEMBER 18, 2007

Mr. CLAY (for himself, Mr. TOWNS, and Mr. WAXMAN) introduced the following bill; which was referred to the Committee on Oversight and Government Reform

---

A BILL

To amend title 44, United States Code, to strengthen requirements for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

(a) SHORT TITLE.—This Act may be cited as the "Federal Agency Data Protection Act".

(b) TABLE OF CONTENTS.—The table of contents of this Act is as follows:

Sec. 1. Short title; table of contents.
Sec. 2. Purpose.
Sec. 3. Definition of personally identifiable information.
Sec. 4. Authority of Director of Office of Management and Budget to establish information security policies and procedures.
Sec. 5. Responsibilities of Federal agencies for information security.
Sec. 6. Protection of government computers from risks of peer-to-peer file sharing.
Sec. 7. Annual independent audit.
Sec. 8. Privacy impact assessment of Federal agency use of commercial information services containing personal information.
Sec. 9. Prohibition on certain contracts with data brokers.
Sec. 10. Authorization of appropriations.
Sec. 11. Implementation.

SEC. 2. PURPOSE.

The purpose of this Act is to protect personally identifiable information of individuals that is maintained in or transmitted by Federal agency information systems.

SEC. 3. DEFINITION OF PERSONALLY IDENTIFIABLE INFORMATION.

Section 3542(b) of title 44, United States Code, is amended by adding at the end the following new paragraph:

"(4) The term 'personally identifiable information', with respect to an individual, means any information about the individual maintained by an agency, including information—

"(A) about the individual's education, finances, or medical, criminal, or employment history;

"(B) that can be used to distinguish or trace the individual's identity, including name,

1 social security number, date and place of birth,
2 mother's maiden name, or biometric records; or
3 "(C) that is linked or linkable to the indi-
4 vidual.".

5 **SEC. 4. AUTHORITY OF DIRECTOR OF OFFICE OF MANAGE-**
6 **MENT AND BUDGET TO ESTABLISH INFORMA-**
7 **TION SECURITY POLICIES AND PROCEDURES.**

8 Section 3543(a) of title 44, United States Code, is
9 amended—
10 (1) by striking "and" at the end of paragraph
11 (7);
12 (2) in paragraph (8)—
13 (A) by striking "and" at the end of sub-
14 paragraph (D);
15 (B) by striking the period and inserting ";
16 and" at the end of subparagraph (E); and
17 (C) by adding at the end the following new
18 subparagraph:
19 "(F) a summary of the breaches of infor-
20 mation security reported by agencies to the Di-
21 rector and the Federal information security in-
22 cident center pursuant to paragraph (10);"; and
23 (3) by adding at the end the following:

"(9) establishing minimum requirements regarding the protection of information maintained in or transmitted by mobile digital devices, including—

"(A) requirements for the protection of personally identifiable information; and

"(B) requirements for—

"(i) the encryption of such information consistent with standards promulgated under section 11331 of title 40; or

"(ii) the use of other commercially available technologies that efficiently and effectively render information unusable by unauthorized persons;

"(10) establishing minimum requirements regarding agency action following a breach of information security resulting in the disclosure of personally identifiable information, including requirements for—

"(A) timely agency reporting of such breach to the Director and the Federal information security incident center required under section 3546; and

"(B) timely agency notification to individuals whose personally identifiable information may have been compromised or accessed during

1 such breach, based on government-wide risk
2 categories established by the Director after con-
3 sultation with agencies and the public that in-
4 clude exemptions from notification requirements
5 where such information can be reasonably de-
6 termined to be unusable by unauthorized per-
7 sons; and
8 "(11) requiring agencies to comply with mini-
9 mally acceptable system configuration requirements
10 consistent with best practices, including checklists
11 developed under section 8(c) of the Cyber Security
12 Research and Development Act (Public Law 107–
13 305; 116 Stat. 2378) by the Director of the Na-
14 tional Institute of Standards and Technology.".

15 **SEC. 5. RESPONSIBILITIES OF FEDERAL AGENCIES FOR IN-**
16 **FORMATION SECURITY.**

17 Section 3544(b) of title 44, United States Code, is
18 amended—
19 (1) in paragraph (2)(D)(iii), by striking "as de-
20 termined by the agency" and inserting "as required
21 by the Director under section 3543(a)(11)";
22 (2) by striking "and" at the end of paragraph
23 (7);
24 (3) by striking the period at the end of para-
25 graph (8) and inserting "; and"; and

1 (4) by adding at the end the following:

2 "(9) plans and procedures for ensuring the ade-
3 quacy of information security protections for sys-
4 tems maintaining or transmitting personally identifi-
5 able information, including requirements for—

6 "(A) maintaining a current inventory of
7 systems maintaining or transmitting such infor-
8 mation;

9 "(B) implementing information security re-
10 quirements for mobile digital devices maintain-
11 ing or transmitting such information, as re-
12 quired by the Director (including encryption or
13 the use of other commercially available tech-
14 nologies rendering data unusable by unauthor-
15 ized persons);

16 "(C) timely reporting of information secu-
17 rity breaches involving such information to the
18 Director and the Federal information security
19 incident center required under section 3546;

20 "(D) timely notification to individuals
21 whose personally identifiable information may
22 have been compromised or accessed during an
23 information security breach, consistent with
24 policies and procedures issued by the Director;
25 and

"(E) developing, implementing, and overseeing remediation plans to address vulnerabilities in information security protections for such information.".

SEC. 6. PROTECTION OF GOVERNMENT COMPUTERS FROM RISKS OF PEER-TO-PEER FILE SHARING.

(a) PLANS REQUIRED.—As part of the Federal agency responsibilities set forth in sections 3544 and 3545 of title 44, United States Code, the head of each agency shall develop and implement a plan to protect the security and privacy of computers and networks of the Federal Government from the risks posed by peer-to-peer file sharing.

(b) CONTENTS OF PLANS.—Such plans shall set forth appropriate methods, including both technological (such as the use of software and hardware) and nontechnological methods (such as employee policies and user training), to achieve the goal of protecting the security and privacy of computers and networks of the Federal Government from the risks posed by peer-to-peer file sharing.

(c) IMPLEMENTATION OF PLANS.—The head of each agency shall—

(1) develop and implement the plan required under this section as expeditiously as possible, but in no event later than six months after the date of the enactment of this Act; and

1 (2) review and revise the plan periodically as
2 necessary.
3 (d) REVIEW OF PLANS.—Not later than 18 months
4 after the date of the enactment of this Act, the Comp-
5 troller General shall—
6 (1) review the adequacy of the agency plans re-
7 quired by this section; and
8 (2) submit to the Committee on Government
9 Reform of the House of Representatives and the
10 Committee on Governmental Affairs of the Senate a
11 report on the results of the review, together with any
12 recommendations the Comptroller General considers
13 appropriate.
14 (e) DEFINITIONS.—In this section:
15 (1) PEER-TO-PEER FILE SHARING.—The term
16 "peer-to-peer file sharing" means the use of com-
17 puter software, other than computer and network
18 operating systems, that has as its primary function
19 the capability to allow the computer on which such
20 software is used to designate files available for
21 transmission to another computer using such soft-
22 ware, to transmit files directly to another such com-
23 puter, and to request the transmission of files from
24 another such computer. The term does not include
25 the use of such software for file sharing between,

among, or within Federal, State, or local government agencies.

(2) AGENCY.—The term "agency" has the meaning provided by section 3502 of title 44, United States Code.

SEC. 7. ANNUAL INDEPENDENT AUDIT.

(a) REQUIREMENT FOR AUDIT INSTEAD OF EVALUATION.—Section 3545 of title 44, United States Code, is amended—

(1) in the section heading, by striking "**evaluation**" and inserting "**audit**" ; and

(2) in paragraphs (1) and (2) of subsection (a), by striking "evaluation" and inserting "audit" both places it appears.

(b) ADDITIONAL SPECIFIC REQUIREMENTS FOR AUDITS.—Section 3545(a) of such title is amended—

(1) in paragraph (2)(A), by striking "subset of the agency's information systems;" and inserting the following: "subset of—

"(i) the information systems used or operated by the agency; and

"(ii) the information systems used, operated, or supported on behalf of the agency by a contractor of the agency, any

1 subcontractor (at any tier) of such a con-
2 tractor, or any other entity;"; and
3 (2) by adding at the end the following new
4 paragraph:
5 "(3) Each audit under this section shall conform to
6 generally accepted government auditing standards.".
7 (c) CONFORMING AMENDMENTS.—
8 (1) Each of the following provisions of section
9 3545 of title 44, United States Code, is amended by
10 striking "evaluation" and inserting "audit" each
11 place it appears:
12 (A) Subsection (b)(1).
13 (B) Subsection (b)(2).
14 (C) Subsection (c).
15 (D) Subsection (e)(1).
16 (E) Subsection (e)(2).
17 (2) Section 3545(d) of such title is amended by
18 striking "the evaluation required by this section"
19 and inserting "the audit required by this section".
20 (3) Section 3545(f) of such title is amended by
21 striking "evaluators" and inserting "auditors".
22 (4) Section 3545(g)(1) of such title is amended
23 by striking "evaluations" and inserting "audits".
24 (5) Section 3545(g)(3) of such title is amended
25 by striking "Evaluations" and inserting "Audits".

(6) Section 3543(a)(8)(A) of such title is amended by striking "evaluations" and inserting "audits".

(7) Section 3544(b)(5)(B) of such title is amended by striking "evaluation" and inserting "audit".

SEC. 8. PRIVACY IMPACT ASSESSMENT OF FEDERAL AGENCY USE OF COMMERCIAL INFORMATION SERVICES CONTAINING PERSONAL INFORMATION.

(a) IN GENERAL.—Section 208(b)(1)(A) of the E-Government Act of 2002 (44 U.S.C. 3501 note) is amended—

(1) by striking "or" at the end of clause (i); and

(2) in clause (ii), by striking the period at the end of subclause (II) and inserting "; or"; and

(3) by inserting after clause (ii) the following:

"(iii) purchasing or subscribing for a fee to information in identifiable form from a data broker.".

(b) DEFINITIONS.—Section 208(d) of such Act (44 U.S.C. 3501 note) is amended to read as follows:

"(d) DEFINITIONS.—In this section:

1 "(1) IDENTIFIABLE FORM.—The term 'identifi-
2 able form' means any representation of information
3 that permits the identity of an individual to whom
4 the information applies to be reasonably inferred by
5 either direct or indirect means.

6 "(2) DATA BROKER.—The term 'data broker'
7 means a business entity that, for monetary fees or
8 dues, regularly engages in the practice of collecting,
9 transmitting, or providing access to sensitive infor-
10 mation in identifiable form on more than 5,000 indi-
11 viduals who are not the customers or employees of
12 that business entity or affiliate primarily for the
13 purposes of providing such information to non-
14 affiliated third parties on an interstate basis.".

15 (c) STUDY.—Not later than 2 years after the date
16 of the enactment of this Act, the Comptroller General of
17 the United States shall submit a report to the Congress
18 regarding Federal agency compliance with the require-
19 ments established by the amendments made by this sec-
20 tion.

21 **SEC. 9. PROHIBITION ON CERTAIN CONTRACTS WITH DATA**
22 **BROKERS.**

23 Section 208 of the E-Government Act of 2002 (44
24 U.S.C. 3501 note) is amended—

1 (1) by redesignating subsection (d) as sub-
2 section (e); and
3 (2) by inserting after subsection (c) the fol-
4 lowing:
5 "(d) PROHIBITION ON CERTAIN CONTRACTS WITH
6 DATA BROKERS.—
7 "(1) PROHIBITION.—Notwithstanding any other
8 provision of law, beginning 1 year after the date of
9 the enactment of this subsection, no Federal agency
10 may enter into a contract with a data broker, or
11 issue a task or delivery order under a contract with
12 a data broker, to access for a fee any database con-
13 sisting primarily of information in identifiable form
14 concerning United States persons (other than a
15 database consisting of news reporting or telephone
16 directories) unless the head of such agency imple-
17 ments the requirements specified in paragraph (2).
18 "(2) REQUIREMENTS.—For purposes of para-
19 graph (1), the requirements specified in this para-
20 graph are the following:
21 "(A) COMPLETION OF PRIVACY IMPACT AS-
22 SESSMENT.—With respect to any database pro-
23 posed to be accessed, the head of the agency
24 shall complete a privacy impact assessment
25 under this section. The assessment shall, sub-

1 ject to the provisions in this section pertaining
2 to sensitive information, include a description
3 of—
4 "(i) such database;
5 "(ii) the name of the data broker
6 from which it is proposed to be obtained;
7 and
8 "(iii) the amount of the contract or
9 task or delivery order proposed to be en-
10 tered into or issued.
11 "(B) PROMULGATION OF REGULATIONS.—
12 The head of the agency shall promulgate regu-
13 lations that specify—
14 "(i) the personnel permitted to access,
15 analyze, or otherwise use databases of the
16 type described in paragraph (1);
17 "(ii) standards governing the access,
18 analysis, or use of such databases;
19 "(iii) any standards used to ensure
20 that the information in identifiable form
21 accessed, analyzed, or used is the minimum
22 necessary to accomplish the intended legiti-
23 mate purpose of the Federal agency;

1 "(iv) standards limiting the retention
2 and redisclosure of information in identifi-
3 able form obtained from such databases;
4 "(v) procedures ensuring that such
5 data meet standards of accuracy, rel-
6 evance, completeness, and timeliness;
7 "(vi) the auditing and security meas-
8 ures to protect against unauthorized ac-
9 cess, analysis, use, or modification of data
10 in such databases;
11 "(vii) applicable mechanisms by which
12 individuals may secure timely redress for
13 any adverse consequences wrongly incurred
14 due to the access, analysis, or use of such
15 databases;
16 "(viii) mechanisms, if any, for the en-
17 forcement and independent oversight of ex-
18 isting or planned procedures, policies, or
19 guidelines; and
20 "(ix) an outline of enforcement mech-
21 anisms for accountability to protect indi-
22 viduals and the public against unlawful or
23 illegitimate access or use of databases.
24 "(C) INCLUSION OF PENALTIES AND
25 OTHER REQUIREMENTS IN LARGER CON-

1 TRACTS.—With respect to any contract or task
2 or delivery order proposed to be entered into or
3 issued in an amount greater than $500,000, the
4 head of the agency shall include in the contract
5 or order the following provisions:
6 "(i) Provisions providing for pen-
7 alties—
8 "(I) for failure to implement a
9 comprehensive personal data privacy
10 and security program that includes
11 administrative, technical, and physical
12 safeguards appropriate to the size and
13 complexity of the business entity and
14 the nature and scope of its activities;
15 or
16 "(II) for the provision to the
17 Federal agency of inaccurate informa-
18 tion in identifiable form, if the entity
19 knows or has reason to know that the
20 information being provided is inac-
21 curate.
22 "(ii) Provisions requiring a data
23 broker that retains service providers for re-
24 sponsibilities related to information in
25 identifiable form to—

"(I) exercise appropriate due diligence in selecting those service providers for responsibilities related to such information;

"(II) take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the security, privacy, and integrity of such information; and

"(III) require such service providers, by contract, to implement a comprehensive personal data privacy and security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the business entity and the nature and scope of its activities.

"(3) LIMITATION ON PENALTIES.—The penalties under paragraph (2)(C)(i) shall not apply to a data broker providing information in identifiable form that is accurately and completely recorded from a public record source.".

1 **SEC. 10. AUTHORIZATION OF APPROPRIATIONS.**

2 Section 3548 of title 44, United States Code, is
3 amended by striking "2007" and inserting "2012".

4 **SEC. 11. IMPLEMENTATION.**

5 Except as otherwise specifically provided in this Act,
6 implementation of this Act and the amendments made by
7 this Act shall begin not later than 90 days after the date
8 of the enactment of this Act.

○

Mr. CLAY. We will now receive testimony from the witnesses before us today. On today's panel, the subcommittees are pleased to have the following witnesses: Karen Evans, Administrator for the Office of E-Government and Information Technology. Ms. Evans is an experienced IT professional and leads the administration's programs on information security. Welcome back to the committee, Ms. Evans.

We also have Greg Wilshusen, Director for Information Security Issues at the Government Accountability Office. Mr. Wilshusen is also a long-time expert and has testified on this topic before the Information Policy Subcommittee several times. Thank you for being here.

Alan Paller is the director of research at the SANS Institute and is responsible for overseeing all research projects. Mr. Paller founded the CIO Institute and earned degrees in computer science and engineering from Cornell and MIT. Welcome to the committee hearing.

Bruce McConnell, the president and founder of McConnell International. Prior to his current position, Mr. McConnell was chief of information and technology policy at the White House Office of Management and Budget, where he led several IT and security initiatives. Thank you for being here, too, Mr. McConnell.

Rounding us out is Tim Bennett, president of Cyber Security Industry Alliance. Mr. Bennett served as the vice VP of the American Electronics Association and worked in senior roles within the Office of the U.S. Trade. Thank you also, Mr. Bennett, for coming today.

I thank all of you for appearing before the subcommittee. It is the policy of the committee to swear in all witnesses before they testify, so I will ask you to please rise and raise your right hands.

[Witnesses sworn.]

Mr. CLAY. Thank you, and let the record reflect that the witnesses answered in the affirmative.

I ask that each witness now give a brief summary of their testimony and to keep the summary under 5 minutes in duration. Bear in mind your complete written statement will be included in the hearing record. I will let you know if you go over the 5. We will start with Ms. Evans. You may proceed.

STATEMENTS OF KAREN S. EVANS, ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY, OFFICE OF MANAGEMENT AND BUDGET; GREGORY C. WILSHUSEN, DIRECTOR, INFORMATION SECURITY ISSUES, GOVERNMENT ACCOUNTABILITY OFFICE; ALAN PALLER, DIRECTOR OF RESEARCH, THE SANS INSTITUTE; BRUCE W. MCCONNELL, PRESIDENT, MCCONNELL INTERNATIONAL, LLC; AND TIM BENNETT, PRESIDENT, CYBER SECURITY INDUSTRY ALLIANCE

STATEMENT OF KAREN S. EVANS

Ms. EVANS. Good morning, Chairman Clay. Thank you for inviting me to speak about the status of the Federal Government's efforts to safeguard our information and systems. My remarks today will highlight a few of the initiatives underway to manage the risk associated with our Government services in this ever-changing IT

environment. The details are included in my written statement. I will conclude with our thoughts on your proposed bill, H.R. 4791.

Information security and privacy are extremely important issues for the administration. On March 1st, the Office of Management and Budget [OMB], will provide our fifth annual report to Congress on the implementation of the Federal Information Security Management Act [FISMA], which will detail our improvements and remaining weaknesses for both security and privacy.

Over the past year, departments and agencies continue to improve their security programs, manage their risks and become more fully compliant with FISMA. To enhance information security programs, OMB continues to use the oversight mechanisms to improve performance, including the President's management agenda score card and the agencies' capital planning processes. We are also engaging agencies in a variety of information security and privacy initiatives to close any remaining performance gaps.

Over the past year, in collaboration with the National Institute for Standards and Technology [NIST], the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops, which are running Microsoft Windows XP or Vista, known as the Federal Desktop Core Configuration [FDCC]. By implementing a common configuration, we are gaining better control of our Federal desktops, allowing for closer monitoring and correction of potential vulnerabilities. We are also working with the vendor community to make their applications safer.

NIST has developed testing tools for use both by the Federal agencies and the vendors and three independent laboratories have been accredited by NIST's National Voluntary Laboratory Accreditation Program, to provide the validation testing. We are very optimistic this program will greatly enhance the security of our Federal desktops and applications.

To help agency procurement officers with the validation requirement, we are working with the Federal Acquisition Council to incorporate language into the Federal Acquisition Register. Agencies connect to the internet to develop timely information and to deliver services to the public. However, our Government systems are continuously operating under increasing levels of risk. Through the Trusted Internet Connections Initiative, we are working with agencies to reduce the overall number of external Federal connections to manage risk in a more cost-effective and efficient manner, while providing better awareness of our environment. Agencies turned in plans of action and milestones to fully optimize agency connections with a target completion date of June 2008.

Recently, we provided the opportunity for all departments and agencies to review the proposed legislation, H.R. 4791. The bill contains several provisions which aim to enhance the protection of Federal information and personally identifiable information, as well as several provisions that propose changes to FISMA. While we strongly support enhancing protections for such information, we share several concerns expressed across the Federal agencies about the effect of this legislation.

The administration believes the foundation and the framework established by FISMA is sound and also believes there is still much

we can accomplish to improve the security and manage the risk associated with our information and information services. Nonetheless, we are concerned with the unintended consequences of the proposed change which would seriously impact established agency security and privacy practices, while not necessarily achieving the outcomes of improved privacy or security.

While we understand technologies which are improperly implemented introduce increased risk, we recommend any potential changes to the statute be technology-neutral. We recognize that the IT landscape is ever-changing. As we deploy common, Government-wide solutions, departments and agencies increasingly are requiring services instead of procuring infrastructure.

We welcome the opportunity to further discuss potential gaps which may need to be addressed through future FISMA enhancements if appropriate. We look forward to discussing our ongoing information security and privacy activities in greater detail. We feel our current activities and initiatives as included in my written statement already are beginning to close performance gaps H.R. 4791 attempts to address.

I would be happy to answer questions at the appropriate time.

[The prepared statement of Ms. Evans follows:]

STATEMENT OF
THE HONORABLE KAREN EVANS
ADMINISTRATOR FOR ELECTRONIC GOVERNMENT AND INFORMATION TECHNOLOGY
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
HOUSE SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES AND THE SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, ORGANIZATION, AND PROCUREMENT, OF THE COMMITTEE OF OVERSIGHT AND GOVERNMENT REFORM

February 14, 2008

Good morning, Mr. Chairman and Members of the Subcommittee. Thank you for inviting me to speak about the status of the Federal government's efforts to safeguard our information and systems.

My remarks today will focus on the progress we have made in improving the security of the government's information and information technology (IT) systems as well as our strategy for managing the risk associated with our government services in this ever changing IT environment. In our increasingly interconnected and interdependent environment, security risks left unaddressed by one agency can exponentially compound security risks faced by all of us. Weaknesses in information security and privacy programs prevent agencies from achieving program goals and erode the public's trust in us and our services.

Information security and privacy are extremely important issues for the Administration. On March 1st, the Office of Management and Budget (OMB) will provide our fifth annual report to the Congress on implementation of the Federal Information Security Management Act (FISMA). This report will go into detail on our improvements and remaining weaknesses for both security and privacy.

Each year, OMB provides to the agencies specific guidance for reporting on the status and progress of their security programs. We use this data to oversee their programs, evaluate security and privacy overall, and develop our annual FISMA report. As in the past, this year's guidance included both quantitative and qualitative performance measures related to the major provisions of FISMA and to agency privacy program requirements. In addition to the questions and measures included in previous years, this year OMB used the FISMA reporting vehicle to gather Inspectors General's (IG's) assessments of the quality of agency Privacy Impact Assessments (PIAs) processes.

Over the past year, departments and agencies continued to improve their security programs, manage their risk and become more fully compliant with FISMA. An increasing number of agency systems completed certification and accreditation and

annual testing of their security controls. In addition, agency IGs reported improvements in the quality of certification and accreditation and agencies' corrective plans of action and milestones. Agencies continued to improve their privacy programs.

In addition to information security progress, the Federal government has been making progress in implementing the April 2007 recommendations of the President's Identity Theft Task Force. Specifically, we have required agencies to review the use of Social Security Numbers (SSNs), underscored data security guidance – including encryption of portable storage and encryption devices.

On May 22, 2007, OMB issued Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information." M-07-16 required agencies to complete their review for the use of SSNs and to identify instances in which collection or use of the SSN is unnecessary. Within 120 days from the date of the memo, M-07-16 required agencies to establish a plan to eliminate the unnecessary collection and use of SSNs within 18 months. OMB is working with SSA and other agencies to explore alternatives to agency use of SSNs as a personal identifier in Federal programs. For Federal employees, OPM is leading the effort to develop policy for employee identifiers to minimize risk of identify theft.

In addition to M-07-16's requirement to complete the survey for the use of SSNs, the memo included reminders to encrypt all data on mobile computers/devices carrying agency data, unless the data is determined, in writing by the Deputy Secretary of each department, to not to be sensitive. This reminder would include agency laptops and other devices which contain personal information. Per this requirement, the encryption must be the National Institute of Science and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 certified. To implement FIPS 140-2, or Security Requirements for Cryptographic Modules, NIST has developed a testing and certification program to ensure the encryption algorithm being used in the product is secure. All encryption must pass this certification process.

How Do We Oversee Agency Performance?

In addition to the annual FISMA reporting process, OMB continues to use the oversight mechanisms described below to improve agency and government-wide IT security performance.

President's Management Agenda Scorecard

The President's Management Agenda (PMA) Expanding Electronic Government (E-Government) Scorecard includes quarterly reporting on agencies' efforts to meet their security goals. Agencies must provide OMB with a quarterly update on IT security performance measures and Plan of Actions and Milestones (POA&M) progress. The quarterly updates enable the agency and OMB to monitor agency remediation efforts and

identify progress and problems.

Information technology security is one of a number of critical components agencies must implement to get to green (or yellow) for the E-Government scorecard. If the security criteria are not successfully met, agencies cannot improve their status on the scorecard. Agencies are publicly accountable for meeting the government-wide goals, and scores are posted quarterly at http://results.gov/agenda/scorecard.html.

Scorecards are also used to track agency progress in improving privacy programs and practices. In each Agency's Third Quarter of FY 2007 E-government scorecard, OMB included language that required Chief Information Officers (CIOs) to certify compliance with M-07-16. Due to agency difficulties in certifying compliance so shortly after the issuance of M-07-16, OMB required agencies in the Fourth Quarter scorecards to submit a status update by December 14th as well as a date when the agency would be in full compliance of the M-07-16 requirements, such as development of a breach notification policy and incident reporting requirements. The Fourth Quarter scorecards also required CIOs to certify that they had reminded agency staff to protect laptops and other portable data storage and communication devices.

Review of Agency Information Technology Investment Requests

Several years ago, OMB integrated information technology security into the capital planning and investment control process to ensure security was built into and funded over the lifecycle of each agency system. This also helps promote greater management attention to security as a fundamental priority. To guide agency resource decisions and assist oversight, OMB's policies require agencies to:

- Report security costs for all information technology investments;
- Document adequate security controls and costs have been incorporated into the life cycle planning of each investment; and
- Tie the POA&Ms for a system directly to the funding request for the system.

Additionally, agencies must answer a series of security questions and describe how the investment meets the requirements of the FISMA, OMB policy, and the NIST guidelines. The justifications are then evaluated on specific criteria including whether the system's cyber-security, planned or in place, is appropriate.

This year, when reviewing investments, we considered the IG's annual review of the quality of the agency's C&A process. If the process was not considered "satisfactory" or better by the agency IG, the agency's investment portfolio was placed on our Management Watch List to continue the necessary management oversight.

Ongoing Security and Privacy Initiatives

As agencies continue to improve their security and privacy metrics reported quarterly and annually, we are striving to help agencies with their operational security and privacy processes by providing cross-agency tools and collaboration opportunities. Recently, we've engaged agencies in several new initiatives building upon the foundation of the activities associated with FISMA and privacy compliance processes. New and existing initiatives to help agencies improve their security and privacy posture have been well received, and are entering the implementation phase across agencies. These initiatives, which I will discuss in greater depth throughout this testimony, aim to improve security and privacy while allowing agencies to implement requirements in a more cost effective manner.

Federal Desktop Core Configuration (FDCC)

Over the past year, in collaboration with NIST, the Department of Defense, the National Security Agency, and Microsoft, we have developed a set of information security controls to be implemented on all Federal desktops which are running Microsoft Windows XP or VISTA. This set of controls, known as the Federal Desktop Core Configuration (FDCC) is currently being implemented across the Federal enterprise. By implementing a common configuration, we are gaining better control of our Federal systems, and allowing for closer monitoring and correction of potential vulnerabilities. Security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. In particular, security configurations help protect connections to the Internet and limit the download of Internet applications to only authorized professionals.

In addition to the desktop configuration, we are also working with the vendor community to make their applications safer. As part of this program, NIST has developed testing tools for use by both Federal agencies and vendors. NIST awarded Security Content Automation Protocol (SCAP) Validation to three products as of February 4th, 2008. These products and their associated validation information can be found at http://nvd.nist.gov/scapproducts.cfm. Three independent laboratories have been accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) for SCAP Product Validation testing. The list of accredited labs is available at the same URL. We are very optimistic this program will greatly enhance the security of our Federal desktops, and, of our Federal enterprise as a whole. We are requiring agencies use these tested products, and to help agency procurement officers with this requirement, we have provided agencies with recommended procurement language. This language can be found in our Memorandum M-07-18, "Ensuring New Acquisitions Include Common Security Configurations," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf. Currently, the Federal Acquisition Council is in the process of adding similar language to the Federal Acquisition Regulation.

Trusted Internet Connections

Agencies connect to the Internet to deliver timely information and services to the public, however, our Government systems are continuously operating under increasing

levels of risk. Each new external connection increases threats and vulnerabilities faced by agencies, and reports are demonstrating we are experiencing consequences such as loss of public confidence. Through the Trusted Internet Connections (TIC) initiative, we are working with agencies to reduce the overall number of external Federal connections, in order to manage our risk and secure our connections in a more cost-effective and efficient manner to provide better awareness of our environment. Agencies turned in plans of action and milestones to fully optimize agency connections, with a target completion date of June 2008.

As agencies optimize their external connections, security controls to monitor threats must be deployed and correlated to create a government-wide perspective of shared risks to our networks. The Department of Homeland Security (DHS) supports an application named Einstein to collect, analyze, and share aggregated computer security information across the Federal government. Einstein will assist agencies to raise their awareness and DHS for government-wide awareness for information security threats and vulnerabilities. This awareness will enable agencies and DHS to take corrective action in a timely manner. We are currently working with DHS to build upon their existing deployments and extend Einstein to all of the Federal agencies.

Information System Security Line of Business (ISSLOB)

Through the ISSLOB, introduced in the Spring of 2005, an inter-agency task force identified common solutions to be shared across government and developed a joint business case outlining a general concept of operations with overall milestones and budget estimates. The Task Force identified common solutions in four areas: security training; FISMA reporting; situational awareness/incident response; and selection, evaluation and implementation of security solutions. All agencies were asked to submit proposals to either become a Shared Service Center (SSC) for other agencies, or migrate to another agency from which they would acquire expert security services. DHS helped coordinate the selection of SSCs, and agency implementation of these services.

As of November 2007, 12 agencies had implemented security awareness training services provided by the initiative, and 13 agencies had begun using FISMA reporting services provided by the initiative. As a result, agencies are beginning to reduce duplicative investment in common security tools, ensuring a baseline level of training and reporting performance, and are able to refocus their efforts to other complex and critical security issues at their agency. OMB expects agencies will fully report the number of employees trained via the ISSLOB in their fiscal year 2008 annual FISMA report.

With the work completed to date in the ISSLOB, the TIC initiative, implementation of IPv6 and Homeland Security Presidential Directive (HSPD) 12, and the Federal government's initiative to implement the secure desktop configurations (i.e., FDCC), the Federal government is raising the bar of our security posture for our information and IT systems. OMB intends to continue using the ISSLOB to achieve

greater efficiency and effectiveness through standardizing and sharing capabilities, skills, and processes across government, to the maximum extent practicable.

SmartBUY and Blanket Purchase Agreements

SmartBUY is a Federal government procurement vehicle designed to promote effective enterprise level software management. By leveraging the government's immense buying power, SmartBUY can potentially save taxpayers millions of dollars through government wide aggregate buying of Commercial Off the Shelf (COTS) software products. Agencies are utilizing new SmartBUY agreements to acquire quality security products at lower costs. In one recent example, GSA and DOD established a SmartBUY agreement for NIST certified products which will encrypt data at rest. This not only benefits Federal agencies, since the Blanket Purchase Agreement (BPA) was written so that states and local governments can also take advantage of this opportunity.

In addition to the encryption BPA, GSA worked to complete two BPA's for credit monitoring services deemed necessary by an agency in the event of a breach of personally identifiable information (PII), as well as risk assessment services for when a breach occurs. More information about the BPA related to credit monitoring services can be found in our OMB Memorandum M-07-04, "Use of Commercial Credit Monitoring Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2007/m07-04.pdf. More information about the BPA aimed at helping agencies to better respond to PII incidents and breach notifications can be found in our OMB Memorandum M-08-10, "Use of Commercial Independent Risk Analysis Services Blanket Purchase Agreements (BPA)," at http://www.whitehouse.gov/omb/memoranda/fy2008/m08-10.pdf. Currently, the ISSLOB is working across Federal agencies and with GSA, to assess the feasibility of additional security related SmartBUY and BPA opportunities for situational awareness and discovery tool sets.

H.R. 4791

Recently, we provided the opportunity for all departments and agencies to review proposed legislation, H.R. 4791, entitled, "Federal Agency Data Protection Act." The bill contains several provisions that aim to enhance the protection of Federal information and personally identifiable information, as well as several provisions that propose changes to the FISMA. While we strongly support enhancing protections for such information we share several concerns expressed across Federal agencies about the effect of this legislation. The Administration believes the foundation and framework established by FISMA is sound, and also believes that there is still much we can accomplish to improve the security and manage the risk associated with our information and information services. Nonetheless, we are concerned that the unintended consequences of the proposed changes would seriously impact established agency security and privacy practices while not necessarily achieving the outcomes of improved privacy or security. Additionally, while we recognize that technologies that are

improperly implemented introduce increased risk, we recommend any potential changes to the statute be technology-neutral. We recognize that the IT landscape is ever changing. As we deploy common, government-wide solutions, departments and agencies increasingly are acquiring services instead of procuring infrastructure. We welcome the opportunity to further discuss potential gaps that may need to be addressed through future FISMA enhancements, if appropriate. We look forward to discussing our ongoing information security and privacy activities in greater detail. We feel our current activities and initiatives – as described above – already are beginning to close performance gaps H.R. 4791 attempts to address.

Conclusion

Over the past year, agencies made steady progress in closing the Federal government's information and IT systems security performance gaps. Analysis of baseline performance measures indicates policy compliance improvements in a number of programs.

As part of its oversight role, OMB will continue to use quarterly reporting mechanisms along with agency information technology budget planning documents to track key performance metrics for FISMA and privacy compliance. Agency status and progress will be reflected on the President's Management Agenda scorecard.

Finally, the Administration intends to continue our efforts to build upon and provide cross-agency tools and collaboration opportunities through our ongoing information security initiatives. By implementing solid information security solutions across the government, we can address risks and improve security in a cost effective manner. We look forward to your continued support in these areas, and appreciate the attention you've brought to Federal information security and privacy issues.

Mr. CLAY. Thank you, Ms. Evans.

Mr. Wilshusen, you may proceed.

STATEMENT OF GREGORY C. WILSHUSEN

Mr. WILSHUSEN. Mr. Chairman, I am pleased to be here today to testify on FISMA and the state of Federal information security. Rarely has the need for the Federal Government to implement effective controls over its information systems and information been more important. Virtually all Federal operations are supported by automated systems and electronic information, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without them.

At the same time, Federal systems and critical infrastructures are increasingly being targeted for exploitation by a growing array of adversaries, including criminal groups, foreign nation states, hackers, terrorists and disgruntled insiders. Thus, it is imperative that agencies safeguard their systems to protect against such risks as loss or theft to resources, disclosure or modification of sensitive information, including national security, law enforcement, proprietary business and personally identifiable information and disruption of critical operations.

Today, I will summarize agency progress in performing key information security control activities, the effectiveness of information security at Federal agencies, and opportunities to strengthen security. In fiscal year 2007, the Federal Government reported improved security performance relative to key performance metrics established by OMB for FISMA reporting. For example, the percentage of certified and accredited systems Government-wide reportedly increased from 88 percent to 92 percent. These gains continue a historical trend that we reported on last year.

Despite reported progress, 20 of 24 major Federal agencies continue to experience significant information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit or detect access to computer networks, systems or information. Moreover, agencies do not always configure network devices to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, and maintain complete continuity of operations plans for key information systems.

An underlying cause for these weaknesses is that agencies have not fully or effectively implemented the agency-wide information security programs required by FISMA. As a result, Federal systems and information are at increased risk of unauthorized access to and disclosure, modification or destruction of sensitive information as well as the inadvertent or deliberate disruption of system operations and services. Such risks are illustrated in part by an increasing number of security incidents reported by Federal agencies.

Nevertheless, opportunities exist to bolster information security. Federal agencies could implement the hundreds of recommendations made by GAO and agency IGs to resolve previously reported control deficiencies and information security program shortfalls.

In addition, OMB and other Federal agencies have initiated several Government-wide initiatives that are intended to improve security over Federal systems and information. For example, OMB

has established an information systems security line of business to share common processes and functions for managing information system security across Federal agencies, and it has directed agencies to adopt the security configurations developed by NIST, DOD and DHS for certain Windows operating systems. Consideration could also be given to enhancing policies and practices related to security control testing and evaluation, FISMA reporting and the independent annual evaluations of agency information security programs required by FISMA.

In summary, although Federal agencies report performing key control activities on an increasing percentage of their systems, persistent weaknesses in agency information security continues to threaten the confidentiality, integrity and availability of Federal systems and information. Until Federal agencies resolve their significant deficiencies and implement effective security programs, their systems and information will remain at undue and unnecessary risk.

Mr. Chairman, this concludes my statement. I would be happy to answer your questions.

[The prepared statement of Mr. Wilshusen follows:]

United States Government Accountability Office

GAO

Testimony
Before Congressional Subcommittees
Committee on Oversight and Government Reform
House of Representatives

For Release on Delivery
Expected at 11:30 am EST
Thursday, February 14, 2008

INFORMATION SECURITY

Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies

Statement of Gregory C. Wilshusen
Director, Information Security Issues

GAO-08-496T

February 14, 2008

GAO
Accountability · Integrity · Reliability
Highlights

Highlights of GAO-08-496T, a testimony before congressional subcommittees, Committee on Oversight and Government Reform, House of Representatives

INFORMATION SECURITY

Although Progress Reported, Federal Agencies Need to Resolve Significant Deficiencies

Why GAO Did This Study

Information security is especially important for federal agencies, where the public's trust is essential and poor information security can have devastating consequences. Since 1997, GAO has identified information security as a governmentwide high-risk issue in each of its biennial reports to the Congress. Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002, which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies.

GAO was asked to testify on the current state of federal information security and compliance with FISMA. This testimony summarizes (1) agency progress in performing key control activities, (2) the effectiveness of information security at federal agencies, and (3) opportunities to strengthen security. In preparing for this testimony, GAO reviewed prior audit reports; examined federal policies, guidance, and budgetary documentation; and analyzed agency and inspector general (IG) reports on information security.

To view the full product, including the scope and methodology, click on GAO-08-496T. For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Over the past several years, federal agencies consistently reported progress in performing certain information security control activities. According to the President's proposed fiscal year 2009 budget for information technology, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by the Office of Management and Budget (OMB). The percentage of certified and accredited systems governmentwide reportedly increased from 88 percent to 92 percent. Gains were also reported in testing of security controls – from 88 percent of systems to 95 percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that GAO reported on last year.

Despite reported progress, major federal agencies continue to experience significant information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always manage the configuration of network devices to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by an increasing number of security incidents experienced by federal agencies.

Nevertheless, opportunities exist to bolster federal information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information systems security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

Mr. Chairmen and Members of the Subcommittees:

Thank you for the opportunity to participate in today's hearing to discuss information security over federal systems. Information security is a critical consideration for any organization that depends on information systems and computer networks to carry out its mission or business. It is especially important for government agencies, where the public's trust is essential. The need for a vigilant approach to information security is demonstrated by the dramatic increase in reports of security incidents, the wide availability of hacking tools, and steady advances in the sophistication and effectiveness of attack technology. Over the past few years, federal agencies have reported numerous security incidents in which sensitive information has been lost or stolen, including personally identifiable information, which has exposed millions of Americans to a loss of privacy, identity theft, and other financial crimes.

Concerned by reports of significant weaknesses in federal computer systems, Congress passed the Federal Information Security Management Act (FISMA) of 2002,[1] which permanently authorized and strengthened information security program, evaluation, and annual reporting requirements for federal agencies. However, five years after FISMA was enacted, we continue to report that poor information security is a widespread problem with potentially devastating consequences. Since 1997, we have identified information security as a governmentwide high-risk issue in each of our biennial reports to the Congress.[2]

In my testimony today, I will summarize (1) agencies' reported progress in performing key control activities, (2) the effectiveness of information security at federal agencies, including security incidents reported at federal agencies, and (3) opportunities to improve federal information security. In preparing for this testimony, we reviewed prior GAO and agency Inspector General (IG) reports on

[1]FISMA was enacted as title III, E-Government Act of 2002, Pub. L. No.107-347, 116 Stat. 2899, 2946 (Dec. 17, 2002).

[2]Most recently, GAO, *High-Risk Series: An Update*, GAO-07-310 (Washington, D.C.: January 2007).

information security at federal agencies. We also examined fiscal year 2007 governmentwide information security performance information presented in the President's proposed fiscal year 2009 budget for information technology, and information about federal security initiatives; analyzed performance and accountability reports for 24 major federal agencies;[3] and reviewed the Office of Management and Budget's (OMB) FISMA and information technology (IT) security guidance; and information on reported security incidents. We conducted our work, in support of this testimony, during February 2008 in the Washington, D.C. area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Over the past several years, agencies have consistently reported progress in performing certain information security control activities. According to the President's proposed fiscal year 2009 budget for information technology, the federal government continued to improve information security performance in fiscal year 2007 relative to key performance metrics established by OMB. The percentage of certified and accredited systems governmentwide reportedly increased from 88 percent to 92 percent.[4] Gains were also reported in testing of security controls – from 88 percent of systems to 95 percent of systems – and for contingency plan testing – from 77 percent to 86 percent. These gains continue a historical trend that

[3]The 24 major departments and agencies are the Departments of Agriculture, Commerce, Defense, Education, Energy, Health and Human Services, Homeland Security, Housing and Urban Development, the Interior, Justice, Labor, State, Transportation, the Treasury, and Veterans Affairs, the Environmental Protection Agency, General Services Administration, National Aeronautics and Space Administration, National Science Foundation, Nuclear Regulatory Commission, Office of Personnel Management, Small Business Administration, Social Security Administration, and U.S. Agency for International Development.

[4]OMB requires that agency management officials formally authorize their information systems to process information and accept the risk associated with their operation. This management authorization (accreditation) is to be supported by a formal technical evaluation (certification) of the management, operational, and technical controls established in an information system's security plan.

we reported on last year.[5] At that time, agency IGs identified weaknesses in the processes several agencies use to implement these and other security program activities.

Despite the reported progress, federal agencies continue to confront long-standing information security control deficiencies. Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. In addition, agencies did not always effectively manage the configuration of network devices to prevent unauthorized access and ensure system integrity, install patches on key servers and workstations in a timely manner, assign duties to different individuals or groups so that one individual did not control all aspects of a process or transaction, and maintain complete continuity of operations plans for key information systems. An underlying cause for these weaknesses is that agencies have not fully or effectively implemented agencywide information security programs. As a result, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. Such risks are illustrated, in part, by the increasing number of security incidents experienced by federal agencies.

Nevertheless, there are opportunities for federal agencies to bolster information security. Federal agencies could implement the hundreds of recommendations made by GAO and IGs to resolve prior significant control deficiencies and information security program shortfalls. In addition, OMB and other federal agencies have initiated several governmentwide initiatives that are intended to improve security over federal systems and information. For example, OMB has established an information system security line of business to share common processes and functions for managing information systems security and directed agencies to adopt the security configurations developed by the National Institute of Standards and Technology and Departments of Defense and

[5]GAO, *Information Security: Despite Reported Progress, Federal Agencies Need to Address Persistent Weaknesses*, GAO-07-837 (Washington, D.C.: July 27, 2007).

Homeland Security for certain Windows operating systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

Background

Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Therefore, it is important for agencies to safeguard their systems against risks such as loss or theft of resources (such as federal payments and collections), modification or destruction of data, and unauthorized uses of computer resources or to launch attacks on other computer systems. Sensitive information, such as taxpayer data, Social Security records, medical records, and proprietary business information could be inappropriately disclosed, browsed, or copied for improper or criminal purposes. Critical operations could be disrupted, such as those supporting national defense and emergency services or agencies' missions could be undermined by embarrassing incidents, resulting in diminished confidence in their ability to conduct operations and fulfill their responsibilities.

Critical Systems Face Multiple Cyber Threats

Cyber threats to federal systems and critical infrastructures can be unintentional and intentional, targeted or nontargeted, and can come from a variety of sources. Unintentional threats can be caused by software upgrades or maintenance procedures that inadvertently disrupt systems. Intentional threats include both targeted and nontargeted attacks. A targeted attack is when a group or individual specifically attacks a critical infrastructure system. A nontargeted attack occurs when the intended target of the attack is uncertain,

such as when a virus, worm, or malware[6] is released on the Internet with no specific target. The Federal Bureau of Investigation has identified multiple sources of threats to our nation's critical information systems, including foreign nation states engaged in information warfare, domestic criminals, hackers, virus writers, and disgruntled employees working within an organization. Table 1 summarizes those groups or individuals that are considered to be key sources of cyber threats to our nation's information systems and infrastructures.

[6]"Malware" (malicious software) is defined as programs that are designed to carry out annoying or harmful actions. They often masquerade as useful programs or are embedded into useful programs so that users are induced into activating them.

Table 1: Sources of Cyber Threats to Federal Systems and Critical Infrastructures

Threat source	Description
Criminal groups	There is an increased use of cyber intrusions by criminal groups that attack systems for monetary gain.
Foreign nation states	Foreign intelligence services use cyber tools as part of their information gathering and espionage activities. Also, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities. Such capabilities enable a single entity to have a significant and serious impact by disrupting the supply, communications, and economic infrastructures that support military power—impacts that, according to the Director of the Central Intelligence Agency, can affect the daily lives of Americans across the country.[a]
Hackers	Hackers sometimes crack into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites. Thus, attack tools have become more sophisticated and easier to use.
Hacktivists	Hacktivism refers to politically motivated attacks on publicly accessible Web pages or e-mail servers. These groups and individuals overload e-mail servers and hack into Web sites to send a political message.
Disgruntled insiders	The disgruntled insider, working from within an organization, is a principal source of computer crimes. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a victim system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes contractor personnel.
Terrorists	Terrorists seek to destroy, incapacitate, or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the U.S. economy, and damage public morale and confidence. However, traditional terrorist adversaries of the United States are less developed in their computer network capabilities than other adversaries. Terrorists likely pose a limited cyber threat. The Central Intelligence Agency believes terrorists will stay focused on traditional attack methods, but it anticipates growing cyber threats as a more technically competent generation enters the ranks.
Virus writers	Virus writers are posing an increasingly serious threat. Several destructive computer viruses and worms have harmed files and hard drives, including the Melissa macro virus, the Explore.Zip worm, the CIH (Chernobyl) virus, Nimda, and Code Red.

Source: Federal Bureau of Investigation, unless otherwise indicated.

[a]Prepared statement of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, February 2, 2000.

There is increasing concern among both government officials and industry experts regarding the potential for a cyber attack. According to the Director of National Intelligence,[7] "Our information infrastructure—including the internet, telecommunications

[7]*Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence*, Feb. 5, 2008.

networks, computer systems, and embedded processors and controllers in critical industries—increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year."

Increased Vulnerabilities Could Expose Federal Systems to Attack

As federal information systems increase their connectivity with other networks and the Internet and as the system capabilities continue to increase, federal systems will become increasingly more vulnerable. Data from the National Vulnerability Database, the U.S. government repository of standards-based vulnerability management data, showed that, as of February 6, 2008, there were about 29,000 security vulnerabilities or software defects that can be directly used by a hacker to gain access to a system or network. On average, close to 17 new vulnerabilities are added each day. Furthermore, the database revealed that more than 13,000 products contained security vulnerabilities.

These vulnerabilities become particularly significant when considering the ease of obtaining and using hacking tools, the steady advances in the sophistication and effectiveness of attack technology, and the emergence of new and more destructive attacks. Thus, protecting federal computer systems and the systems that support critical infrastructures has never been more important.

Federal Law and Policy Established Federal Information Security Requirements

Over five years have passed since Congress enacted FISMA, which sets forth a comprehensive framework for ensuring the effectiveness of security controls over information resources that support federal operations and assets. FISMA's framework creates a cycle of risk management activities necessary for an effective security program, and these activities are similar to the principles noted in our study of the risk management activities of leading

private sector organizations[8]—assessing risk, establishing a central management focal point, implementing appropriate policies and procedures, promoting awareness, and monitoring and evaluating policy and control effectiveness. More specifically, FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems used or operated by the agency or on behalf of the agency. In this regard, FISMA requires that agencies implement information security programs that, among other things, include

- periodic assessments of the risk;
- risk-based policies and procedures;
- subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;
- security awareness training for agency personnel, including contractors and other users of information systems that support the operations and assets of the agency;
- periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, performed with a frequency depending on risk, but no less than annually;
- a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies;
- procedures for detecting, reporting, and responding to security incidents; and
- plans and procedures to ensure continuity of operations.

[8]GAO, *Executive Guide: Information Security Management Learning From Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May, 1998).

In addition, agencies must develop and maintain an inventory of major information systems that is updated at least annually and report annually to the Director of OMB and several Congressional Committees on the adequacy and effectiveness of their information security policies, procedures, and practices and compliance with the requirements of the act.

OMB and agency IGs also play key roles under FISMA. Among other responsibilities, OMB is to develop policies, principles, standards, and guidelines on information security and is required to report annually to Congress on agency compliance with the requirements of the act. OMB has provided instructions to federal agencies and their IGs for annual FISMA reporting. OMB's reporting instructions focus on performance metrics related to the performance of key control activities such as certifying and accrediting systems, testing and evaluating security controls, and providing security training to personnel. Its yearly guidance also requires agencies to identify any physical or electronic incidents involving the loss of, or unauthorized access to, personally identifiable information.

FISMA also requires agency IGs to perform an independent evaluation of the information security programs and practices of the agency to determine the effectiveness of such programs and practices. Each evaluation is to include (1) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems and (2) assessing compliance (based on the results of the testing) with FISMA requirements and related information security policies, procedures, standards, and guidelines. These required evaluations are then submitted by each agency to OMB in the form of an OMB-developed template that summarizes the results. In addition to the template submission, OMB encourages agency IGs to provide any additional narrative in an appendix to the report to the extent they provide meaningful insight into the status of the agency's security or privacy program.

Agencies Report Progress in Performing Control Activities

Federal agencies continue to report progress in implementing key information security activities. The President's proposed fiscal year 2009 budget for IT states that the federal government continues to improve information security performance relative to the certification and accreditation of systems and the testing of security controls and contingency plans. According to the budget, in 2007 the percentage of certified and accredited systems rose from 88 percent to 92 percent. Even greater gains were reported in testing of security controls—from 88 percent of systems to 95 percent of systems—and for contingency plan testing—from 77 percent to 86 percent.

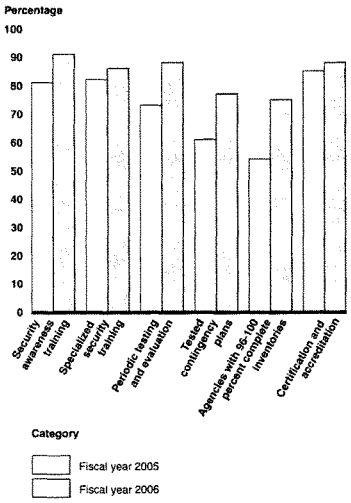
The proposed budget also noted improvements related to agency IG qualitative assessments of certain IT security processes. It reported that the overall quality of the certification and accreditation processes as determined by agency IGs increased compared to 2006, with 76 percent of agencies reporting "satisfactory" or better processes, up from 60 percent the prior year. In addition, the budget noted that 76 percent of agencies demonstrated that they had an effective process in place for identifying and correcting weaknesses using Plans of Action and Milestone management processes.

Although we have not yet verified the information security performance information for fiscal year 2007 contained in the President's proposed budget, the information is consistent with historical trends. As we reported last year, agencies reported increased percentages in most OMB performance metrics for fiscal year 2006 when compared to fiscal year 2005 (see fig. 1) including those related to:

- Percentage of employees and contractors receiving IT security awareness training,
- Percentage of employees with significant security responsibilities who received specialized security training,
- Percentage of systems whose controls were tested and evaluated,

- Percentage of systems with tested contingency plans,
- Percentage of 24 major agencies with 96-100 percent complete inventories of major information systems, and
- Percentage of systems certified and accredited.

Figure 1: Reported Data for Selected Performance Metrics for 24 Major Agencies



Source: GAO analysis of agency FISMA reports.

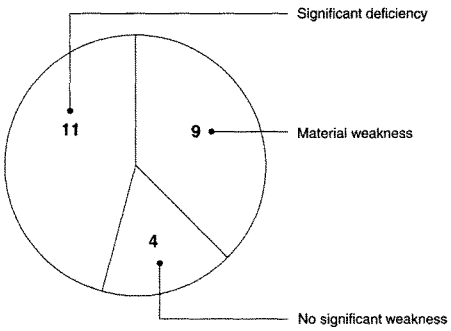
However, for the fiscal year 2006 reporting period, IGs identified weaknesses with their agencies' implementations of those key control activities. For example, according to agency IGs, five major agencies reported challenges in ensuring that contractors had received security awareness training. In addition, they reported that not all systems had been tested and evaluated at least annually, including some high impact systems, and that weaknesses existed in agencies' monitoring of contractor systems or facilities. They highlighted other weaknesses such as contingency plans not being completed for critical systems and inventories of systems that were incomplete. Furthermore, IGs reported weaknesses in agencies' certification and accreditation processes, a key activity OMB uses to monitor agencies' implementation of information security requirements.

Despite Reported Progress, Significant Control Deficiencies Persist at Federal Agencies

Our work and that of IGs show that significant weaknesses continue to threaten the confidentiality, integrity, and availability of critical information and information systems used to support the operations, assets, and personnel of federal agencies. In their fiscal year 2007 performance and accountability reports, 20 of 24 major agencies indicated that inadequate information security controls were either a significant deficiency or a material weakness (see fig. 2).[9] Our audits continue to identify similar conditions in both financial and non-financial systems, including agencywide weaknesses as well as weaknesses in critical federal systems.

[9]A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected.

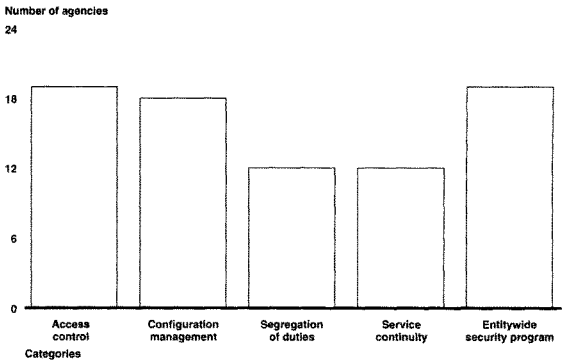
Figure 2: Number of Major Agencies Reporting Significant Deficiencies in Information Security



Source: GAO analysis of agency performance and accountability reports for FY2007.

Persistent weaknesses appear in five major categories of information system controls: (1) access controls, which ensure that only authorized individuals can read, alter, or delete data; (2) configuration management controls, which provide assurance that only authorized software programs are implemented; (3) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (4) continuity of operations planning, which provides for the prevention of significant disruptions of computer-dependent operations; and (5) an agencywide information security program, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented. Figure 3 shows the number of major agencies with weaknesses in these five areas.

Figure 3: Number of Major Agencies Reporting Weaknesses in Control Categories



Source: GAO analysis of agency performance and accountability reports for FY2007.

Access Controls Were Not Adequate

A basic management control objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion of the data. Access controls, which are intended to prevent, limit, and detect unauthorized access to computing resources, programs, information, and facilities, can be both electronic and physical. Electronic access controls include use of passwords, access privileges, encryption, and audit logs. Physical security controls are important for protecting computer facilities and resources from espionage, sabotage, damage, and theft.

Most agencies did not implement controls to sufficiently prevent, limit, or detect access to computer networks, systems, or information. Our analysis of IG, agency, and our own reports uncovered that agencies did not have adequate controls in place to ensure that only authorized individuals could access or manipulate data on their systems and networks. To illustrate, 19 of 24 major agencies reported weaknesses in such controls. For example,

agencies did not consistently (1) identify and authenticate users to prevent unauthorized access, (2) enforce the principle of least privilege to ensure that authorized access was necessary and appropriate, (3) establish sufficient boundary protection mechanisms, (4) apply encryption to protect sensitive data on networks and portable devices, and (5) log, audit, and monitor security-relevant events. Agencies also lacked effective controls to restrict physical access to information assets. We previously reported that many of the data losses occurring at federal agencies over the past few years were a result of physical thefts or improper safeguarding of systems, including laptops and other portable devices.

Weaknesses Also Existed in Other Controls

In addition to access controls, other important controls should be in place to protect the confidentiality, integrity, and availability of information. These controls include the policies, procedures, and techniques for ensuring that computer hardware and software are configured in accordance with agency policies and that software patches are installed in a timely manner; appropriately segregating incompatible duties; and establishing plans and procedures to ensure continuity of operations for systems that support the operations and assets of the agency.

However, agencies did not always configure network devices and services to prevent unauthorized access and ensure system integrity, patch key servers and workstations in a timely manner, or segregate incompatible duties to different individuals or groups so that one individual does not control all aspects of a process or transaction. Furthermore, agencies did not always ensure that continuity of operations plans contained all essential information. Weaknesses in these areas increase the risk of unauthorized use, disclosure, modification, or loss of information.

Agencywide Security Programs Were Not Fully Implemented

An underlying cause for information security weaknesses identified at federal agencies is that they have not yet fully or effectively implemented all the FISMA-required elements for an agencywide information security program. An agencywide security program,

required by FISMA, provides a framework and continuing cycle of activity for assessing and managing risk, developing and implementing security policies and procedures, promoting security awareness and training, monitoring the adequacy of the entity's computer-related controls through security tests and evaluations, and implementing remedial actions as appropriate. Our analysis determined that 19 of 24 major federal agencies had not fully implemented agencywide information security programs. Our recent reports illustrate that agencies often did not adequately design or effectively implement policies for elements key to an information security program.

We identified weaknesses in information security program activities, such as agencies' risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. For example,

- One agency's risk assessment was completed without the benefit of an inventory of all the interconnections between it and other systems. In another case, an agency had assessed and categorized system risk levels and conducted risk assessments, but did not identify many of the vulnerabilities we found and had not subsequently assessed the risks associated with them.
- Agencies had developed and documented information security policies, standards, and guidelines for information security, but did not always provide specific guidance for securing critical systems or implement guidance concerning systems that processed Privacy Act-protected data.
- Security plans were not always up-to-date or complete.
- Agencies did not ensure all information security employees and contractors, including those who have significant information security responsibilities, received sufficient training.
- Agencies had tested and evaluated information security controls, but their testing was not always comprehensive and did not identify many of the vulnerabilities we identified.

- Agencies did not consistently document weaknesses or resources in remedial action plans.

As a result, agencies do not have reasonable assurance that controls are implemented correctly, operating as intended, or producing the desired outcome with respect to meeting the security requirements of the agency, and responsibilities may be unclear, misunderstood, and improperly implemented. Furthermore, agencies may not be fully aware of the security control weaknesses in their systems, thereby leaving their information and systems vulnerable to attack or compromise. Consequently, federal systems and information are at increased risk of unauthorized access to and disclosure, modification, or destruction of sensitive information, as well as inadvertent or deliberate disruption of system operations and services. In prior reports, we and the IGs have made hundreds of recommendations to agencies to address specific information security control weaknesses and program shortfalls. Until agencies effectively and fully implement agencywide information security programs, including addressing the hundreds of recommendations that we and IGs have made, federal information and information systems will not be adequately safeguarded to prevent their disruption, unauthorized use, disclosure, or modification.

Incidents at Federal Agencies Place Sensitive Information and Systems at Risk

The need for effective information security policies and practices is further illustrated by the number of security incidents experienced by federal agencies that put sensitive information at risk. Personally identifiable information about millions of Americans has been lost, stolen, or improperly disclosed, thereby potentially exposing those individuals to loss of privacy, identity theft, and financial crimes. Reported attacks and unintentional incidents involving critical infrastructure systems demonstrate that a serious attack could be devastating. Agencies have experienced a wide range of incidents involving data loss or theft, computer intrusions, and privacy breaches, underscoring the need for improved security practices.

These incidents illustrate that a broad array of federal information and critical infrastructures are at risk.

- The Department of Veterans Affairs (VA) announced that computer equipment containing personally identifiable information on approximately 26.5 million veterans and active duty members of the military was stolen from the home of a VA employee. Until the equipment was recovered, veterans did not know whether their information was likely to be misused. In June, VA sent notices to the affected individuals that explained the breach and offered advice concerning steps to reduce the risk of identity theft. The equipment was eventually recovered, and forensic analysts concluded that it was unlikely that the personal information contained therein was compromised.

- The Transportation Security Administration (TSA) announced a data security incident involving approximately 100,000 archived employment records of individuals employed by the agency from January 2002 until August 2005. An external hard drive containing personnel data, such as Social Security number, date of birth, payroll information, and bank account and routing information, was discovered missing from a controlled area at the TSA Headquarters Office of Human Capital.

- A contractor for the Centers for Medicare and Medicaid Services reported the theft of one of its employee's laptop computer from his office. The computer contained personal information including names, telephone numbers, medical record numbers, and dates of birth of 49,572 Medicare beneficiaries.

- The Census Bureau reported 672 missing laptops, of which 246 contained some degree of personal data. Of the missing laptops containing personal information, almost half (104) were stolen, often from employees' vehicles, and another 113 were not returned by former employees. The Commerce Department reported that employees had not been held accountable for not returning their laptops.

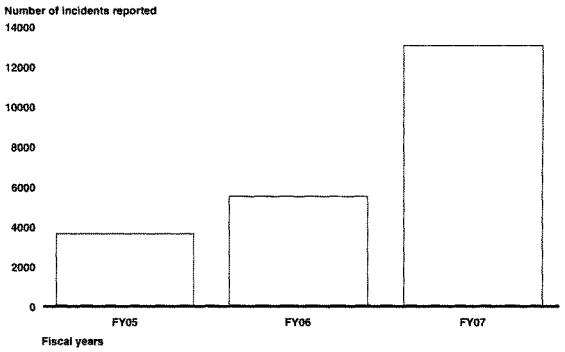
- The Department of State experienced a breach on its unclassified network, which daily processes about 750,000 e-mails and instant messages from more than 40,000 employees and contractors at 100 domestic and 260 overseas locations. The breach involved an e-mail containing what was thought to be an innocuous attachment.

However, the e-mail contained code to exploit vulnerabilities in a well-known application for which no security patch existed. Because the vendor was unable to expedite testing and deploy a new patch, the department developed its own temporary fix to protect systems from being further exploited. In addition, the department sanitized the infected computers and servers, rebuilt them, changed all passwords, installed critical patches, and updated their anti-virus software.

- In August 2006, two circulation pumps at Unit 3 of the Tennessee Valley Authority's Browns Ferry nuclear power plant failed, forcing the unit to be shut down manually. The failure of the pumps was traced to excessive traffic on the control system network, possibly caused by the failure of another control system device.
- Officials at the Department of Commerce's Bureau of Industry and Security discovered a security breach in July 2006. In investigating this incident, officials were able to review firewall logs for an 8-month period prior to the initial detection of the incident, but were unable to clearly define the amount of time that perpetrators were inside its computers, or find any evidence to show that data was lost as a result.
- The Nuclear Regulatory Commission confirmed that in January 2003, the Microsoft SQL Server worm known as "Slammer" infected a private computer network at the idled Davis-Besse nuclear power plant in Oak Harbor, Ohio, disabling a safety monitoring system for nearly 5 hours. In addition, the plant's process computer failed, and it took about 6 hours for it to become available again.

When incidents such as these occur, agencies are to notify the federal information security incident center—US-CERT. As shown in figure 4, the number of incidents reported by federal agencies to US-CERT has increased dramatically over the past 3 years, increasing from 3,634 incidents reported in fiscal year 2005 to 13,029 incidents in fiscal year 2007, (about a 259 percent increase).

Figure 4: Incidents Reported to US-CERT in Fiscal Years 2005 through 2007



Source: GAO analysis of US-CERT data.

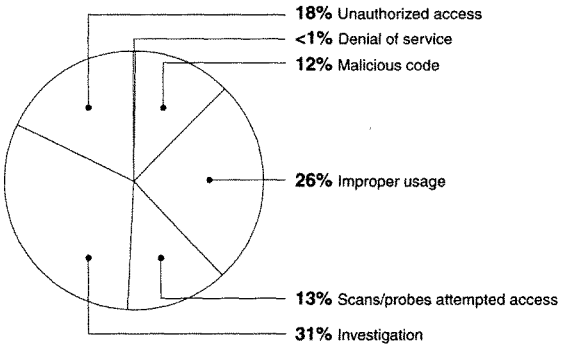
Incidents are categorized by US-CERT in the following manner:

- Unauthorized access: In this category, an individual gains logical or physical access without permission to a federal agency's network, system, application, data, or other resource.
- Denial of service: An attack that successfully prevents or impairs the normal authorized functionality of networks, systems, or applications by exhausting resources. This activity includes being the victim or participating in a denial of service attack.
- Malicious code: Successful installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are not required to report malicious logic that has been successfully quarantined by antivirus software.
- Improper usage: A person violates acceptable computing use policies.

- Scans/probes/attempted access: This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination of these for later exploit. This activity does not directly result in a compromise or denial of service.
- Investigation: Unconfirmed incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review.

As noted in figure 5, the three most prevalent types of incidents reported to US CERT in fiscal year 2007 were unauthorized access, improper usage, and investigation.

Figure 5. Percentage of Incidents Reported to US-CERT in FY07



Source: GAO analysis of US-CERT data.

Opportunities Exist for Enhancing Federal Information Security

In prior reports, GAO and IGs have made hundreds of recommendations to agencies for actions necessary to resolve prior

significant control deficiencies and information security program shortfalls. For example, we recommended agencies correct specific information security deficiencies related to user identification and authentication, authorization, boundary protections, cryptography, audit and monitoring and physical security. We have also recommended that agencies fully implement comprehensive, agencywide information security programs by correcting weaknesses in risk assessments, information security policies and procedures, security planning, security training, system tests and evaluations, and remedial actions. The effective implementation of these recommendations will strengthen the security posture at these agencies.

In addition, recognizing the need for common solutions to improving security, OMB and certain federal agencies have continued or launched several government wide initiatives that are intended to enhance information security at federal agencies. These key initiatives are discussed below.

- *The Information Systems Security Line of Business*: The goal of this initiative is to improve the level of information systems security across government agencies and reduce costs by sharing common processes and functions for managing information systems security. Several agencies have been designated as service providers for IT security awareness training and FISMA reporting.
- *Federal Desktop Core Configuration:* This initiative directs agencies that have Windows XP deployed and plan to upgrade to Windows Vista operating systems to adopt the security configurations develop by NIST, DOD, and DHS. The goal of this initiative is to improve information security and reduce overall IT operating costs.
- *SmartBUY:* This program, led by GSA, is to support enterprise-level software management through the aggregate buying of commercial software governmentwide in an effort to achieve cost savings through volume discounts. The SmartBUY initiative was expanded to include commercial off-the-shelf encryption software and to permit all federal agencies to participate in the program. The initiative is to also include licenses for information assurance.

- *Trusted Internet Connections initiative:* This is an effort designed to optimize individual agency network services into a common solution for the federal government. The initiative is to facilitate the reduction of external connections, including Internet points of presence, to a target of fifty.

In addition to these initiatives, OMB has issued several policy memorandums over the past two years to help agencies protect sensitive data. For example, it has sent memorandums to agencies to reemphasize their responsibilities under law and policy to (1) appropriately safeguard sensitive and personally identifiable information, (2) train employees on their responsibilities to protect sensitive information, and (3) report security incidents. In May 2007, OMB issued additional detailed guidelines to agencies on safeguarding against and responding to the breach of personally identifiable information, including developing and implementing a risk-based breach notification policy, reviewing and reducing current holdings of personal information, protecting federal information accessed remotely, and developing and implementing a policy outlining the rules of behavior, as well as identifying consequences and potential corrective actions for failure to follow these rules.

Opportunities also exist to enhance policies and practices related to security control testing and evaluation, FISMA reporting, and the independent annual evaluations of agency information security programs required by FISMA.

- *Clarify requirements for testing and evaluating security controls.* Periodic testing and evaluation of information security controls is a critical element for ensuring that controls are properly designed, operating effectively, and achieving control objectives. FISMA requires that agency information security programs include the testing and evaluation of the effectiveness of information security policies, procedures, and practices, and that such tests be performed with a frequency depending on risk, but no less than annually.

We previously reported[10] that federal agencies had not adequately designed and effectively implemented policies for periodically testing and evaluating information security controls. Agency policies often did not include important elements for performing effective testing such as how to determine the frequency, depth, and breadth of testing according to risk. In addition, the methods and practices for at six test case agencies were not adequate to ensure that assessments were consistent, of similar quality, or repeatable. For example, these agencies did not define the assessment methods to be used when evaluating security controls, did not test controls as prescribed, and did not include previously reported remedial actions or weaknesses in their test plans to ensure that they had been addressed. In addition, our audits of information security controls often identify weaknesses that agency or contractor personnel who tested the controls of the same systems did not identify. Clarifying or strengthening federal policies and requirements for determining the frequency, depth, and breadth of security controls according to risk could help agencies better assess the effectiveness of the controls protecting the information and systems supporting their programs, operations, and assets.

- *Enhance FISMA reporting requirements.* Periodic reporting of performance measures for FISMA requirements and related analyses provides valuable information on the status and progress of agency efforts to implement effective security management programs.

  In previous reports, we have recommended that OMB improve FISMA reporting by clarifying reporting instructions and requesting IGs to report on the quality of additional performance metrics. OMB has taken steps to enhance its reporting instructions. For example, OMB added questions regarding incident detection and assessments of system inventory. However, the current metrics do not measure how effectively agencies are performing various activities. Current performance measures offer limited assurance of the quality of agency processes that implement key security policies, controls, and practices. For example, agencies are required to test and evaluate

[10]GAO, *Information Security, Agencies Need to Develop and Implement Adequate Policies for Periodic Testing*, GAO-07-65 (Washington, D.C.: Oct. 20, 2006).

the effectiveness of the controls over their systems at least once a year and to report on the number of systems undergoing such tests. However, there is no measure of the quality of agencies' test and evaluation processes. Similarly, OMB's reporting instructions do not address the quality of other activities such as risk categorization, security awareness training, intrusion detection and prevention, or incident reporting. OMB has recognized the need for assurance of quality for agency processes. For example, it specifically requested that the IGs evaluate the certification and accreditation process. The qualitative assessments of the process allows the IG to rate its agency's certification and accreditation process using the terms "excellent," "good," "satisfactory," "poor," or "failing." Providing information on the quality of the processes used to implement key control activities would further enhance the usefulness of the annually reported data for management and oversight purposes.

We also previously reported that OMB's reporting guidance and performance measures did not include complete reporting on certain key FISMA-related activities. For example, FISMA requires each agency to include policies and procedures in its security program that ensure compliance with minimally acceptable system configuration requirements, as determined by the agency. In our report on patch management,[11] we stated that maintaining up-to-date patches is key to complying with this requirement. As such, we recommended that OMB address patch management in its FISMA reporting instructions. Although OMB addressed patch management in its 2004 FISMA reporting instructions, it no longer requests this information. As a result, OMB and the Congress lack information that could identify governmentwide issues regarding patch management. This information could prove useful in demonstrating whether or not agencies are taking appropriate steps for protecting their systems.

- *Consider conducting FISMA-mandated annual independent evaluations in accordance with audit standards or a common approach and framework.* We previously reported that the annual IG

[11]GAO, *Information Security: Continued Action Needed to Improve Software Patch Management*, GAO-04-706 (Washington, D.C.: June 2, 2004).

FISMA evaluations lacked a common approach and that the scope and methodology of the evaluations varied across agencies. For example:

- IGs stated that they were unable to conduct evaluations of their respective agency's inventory because the information provided to them by the agency at that time was insufficient (i.e. incomplete or unavailable).
- IGs reported interviewing officials and reviewing agency documentation, while others indicated conducting tests of implementation plans (e.g. security plans).
- IGs indicated in the scope and methodology sections of their reports that their reviews were focused on selected components, whereas others did not make any reference to the breadth of their review.
- Reports were solely comprised of a summary of relevant information security audits conducted during the fiscal year, while others included additional evaluation that addressed specific FISMA-required elements, such as risk assessments and remedial actions.
- The percentage of systems reviewed was varied. Twenty-two of 24 IGs tested the information security program effectiveness on a subset of systems; two IGs did not review any systems.
- One IG noted that the agency's inventory was missing certain web applications and concluded that the agency's inventory was only 0-50 percent complete, although the report also noted that, due to time constraints, the IG had been unable to determine whether other items were missing.
- Two IGs indicated basing a portion of their template submission solely on information provided to them by the agency, without conducting further investigation.

As we previously reported, the lack of a common methodology, or framework, had culminated in disparities in audit scope, methodology, and content of the IGs' annual independent

evaluations. As a result, the collective IG community may be performing their evaluations without optimal effectiveness and efficiency. Conducting the evaluations in accordance with generally accepted government auditing standards and/or a commonly used framework or methodology could provide improved effectiveness, increased efficiency, quality control, and consistency in assessing whether the agency has an effective information security program. IGs may be able to use the framework to be more efficient by focusing evaluative procedures on areas of higher risk and by following an integrated approach designed to gather evidence efficiently. Having a documented methodology may also offer quality control by providing a standardized methodology, which can help the IG community obtain consistency of application.

In summary, agencies have reported progress in implementing control activities, but persistent weaknesses in agency information security controls threaten the confidentiality, integrity, and availability of federal information and information systems, as illustrated by the increasing number of reported security incidents. Opportunities exist to improve information security at federal agencies. OMB and certain federal agencies have initiated efforts that are intended to strengthen the protection of federal information and information systems. Opportunities also exist to enhance policies and practices related to security control testing and evaluation and FISMA reporting. Similarly, a consideration for strengthening the statutory requirement for the independent annual evaluations of agency information security programs required by FISMA could include requiring IGs to conduct the evaluation in accordance with generally accepted government auditing standards. Until such opportunities are seized and fully exploited and the hundreds of GAO and IG recommendations to mitigate information security control deficiencies and implement agencywide information security programs are fully and effectively implemented, federal information and systems will remain at undue and unnecessary risk.

Mr. Chairmen and Members of the Subcommittees, this concludes my statement. I would be happy to answer questions at this time.

Contact and Acknowledgments

If you have any questions regarding this report, please contact Gregory C. Wilshusen, Director, Information Security Issues, at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this report include Nancy DeFranceso (Assistant Director), Larry Crosland, Neil Doherty, Nancy Glover, Rebecca LaPaze, Stephanie Lee, and Jayne Wilson.

Mr. CLAY. Thank you so much, Mr. Wilshusen.

Mr. Paller.

STATEMENT OF ALAN PALLER

Mr. PALLER. Thank you, and thank you for having me.

I have been to St. Louis a bunch of times, first with McDonnell Douglas and later with Boeing. It is a wonderful, high-tech city.

Mr. CLAY. Thank you so much.

Mr. PALLER. It is very impressive. Actually, what we are talking about today directly affects Boeing, too, so it is not just a Federal discussion because of the change that our other witnesses mentioned.

I am just going to tell you a couple of stories. First of all, I am the research director at SANS, so we have about 68,000 people who are alumni who actually run security at most large organizations. Their job is almost completely impossible. It just isn't out in the public, but we are losing this war against cyber-crime at an accelerating rate, meaning we are falling farther behind every week.

What we are talking about today actually will make a difference. It is not something nice to do for Federal agencies, it actually is a major war, it is involving espionage, it is involving a lot of things that deserve to be treated with more attention. I am here actually with the hope that you can do that by making the Federal Government lead by example. So where the Federal Government uses its procurement, you mentioned in your opening statement $70 billion, that is enough to do an amazing amount of good in security. You don't actually spend the money on security, you use the leverage of the Federal procurement to make the change.

Just to clarify how FISMA became a compliance exercise instead of a security exercise, it wasn't the way the law was intended. It actually was a mistake that was made in GISRA before it became FISMA, the original law that got changed, it was written in the Senate and got changed into FISMA. What happened was that NIST wrote a catalog of things that every agency had to do. They don't even call it a road map or a blue print. They wrote a catalog. And then the IGs and others said, well, now you have to do everything in the catalog. And the problem is, if you had a catalog of things your kids had to do, and one of them was finish their homework and another one was check on the dog, but they were graded on how many things they did, they are going to do all the check on the dogs quick, because the do your homework is hard. And that is what happened with FISMA, because they got graded on how many things they did instead of the important things.

So the leaders are smart, you guys, between Karen and the Hill, you guys made it impossible for them not to do everything. They got Fs on all their report cards. And because of that, they are smart enough to know, they have to get you off their back. So the CIO said, I don't care what you need to do for security, you have to get those reports done, because I have to go see Clay Johnson in the White House and he is going to—well, what they said isn't public. But he will do bad things to me if I don't get all my systems certified.

So the key change, it is a very small change, I have provided your staff with some language that might be better, it will be made

better by your people. But the key change is to prioritize. If homework is more important than checking on the dog, don't say you are going to do these 500 things, say, do your homework. Then if you get your homework done, then do these other things and we will give you bonuses for the other things. But let's make sure we prioritize the actions.

That is what the companies that do security well do. It is all attack-based. They find out where the attacks are coming in, then make sure their defenses can stop those attacks. We don't do that in the Federal Government. So I put all that in the statement.

I want to tell you one more story, because it is a "Karen is a hero" story, and it is really quite a good story. It is the other half of what you can do. John Gilligan was the CIO at the Air Force, he got up in front of 200 people and said, we can't secure our Windows boxes. In fact, we spend more money to clean up after the mess than we do to buy this stuff in the first place, and I am going to change that. He took $500 million over 7 years, so it is not much per year. That is relative to your $70 billion you are talking about. This is the example of how your money makes a difference, $500 million over 7 years.

He said to Microsoft, hey, we want you to configure the system securely when you sell it to us instead of selling it to us open and making every one of our people try to do it after we buy it. And he got it done. Over 400,000 systems now are out of the box secure. The key is, they just reported this, they cut the patching time from 7 weeks to 3 days. And all the attacks come out in the first few days. So if you don't get it done fast, you might as well not patch at all. And they saved tens of millions of dollars. It is the only example where you save money and you improve security. It is what you can do with the leverage you have in your money.

So I am happy to answer questions about any of this. Thank you for letting me come.

[The prepared statement of Mr. Paller follows:]

Statement of
Alan Paller
Director of Research, The SANS Institute
Before The House Subcommittee on Information Policy, Census, and National Archives and the Subcommittee on Government Management, Organization, and Procurement, of the Committee of Oversight and Government Reform
February 14, 2008

Summary

- Federal agencies are under massive attack from China and other nation states, and agencies have demonstrated that they are not able to protect their systems or the sensitive information stored on those systems.
- In 2000, President Clinton vowed to make the federal government leads by example in cyber security.
- Government has failed to lead in large measure because of a provision that was originally made in the Government Information Security Reform Act (GISRA), but carried over to the Federal Information Security Management Act (FISMA). Federal cyber security has been set back, and more than $300 million in scarce cyber security funding has been wasted because of this error.
- A small legislative change and a shift in oversight technique could turn this situation around.
- Time is of the essence. The Director of National Intelligence reported last week to the Senate Select Committee on Intelligence, that cyber exploitation is growing *"more sophisticated, more targeted, and more serious."*

My name is Alan Paller; I am director of research at the SANS Institute. Thank you for the opportunity to testify today. While there are doubtless many things that could be done to improve the security of the Federal government's cyber infrastructure, my testimony today will focus on one item that, in my professional opinion, would materially improve the security of that infrastructure without requiring the expenditure of more money.

The Cyber Threat Is Expanding and Growing In Sophistication

Federal agencies and government contractors are facing a wave of cyber attacks from sophisticated nation states. The attacks began in earnest at least five years ago (our first firm evidence is from May 2003) and are so successful that agencies that know they were penetrated do not know how much information was taken, how widespread the compromises were on their systems, nor which systems are still under control of the attackers.

Those attacks resulted in sensitive data about national security technologies and strategies and practices being copied and moved to hostile nations. The stolen data, although not classified, is highly sensitive – such as details on the technologies that the US considers too sensitive to export and the specifications for the aviation-mission-planning system for Army helicopters, as well as Falconview 3.2, the flight-planning software used by the Army and Air Force. The Commander of the US Air Force Cyber Command, Major General William Lord, said in August of 2006 that "There is a nation-state threat by the Chinese… China has downloaded 10 to 20 terabytes of data from the NIPRNet[1]."
Moreover, the fact that federal computers are under the control of potentially hostile foreign governments means that the US government agencies cannot be sure the data they provide is accurate or whether it may have been altered to be misleading.

[1] NIPRNet is the computer network used by the Department of Defense for unclassified information transfer.

The attacks are continuing, accelerating, and spreading to the commercially owned US critical infrastructure. A week ago today, the Director of National Intelligence, J. Michael McConnell, told the Senate Select Committee on Intelligence,

> *"Our information infrastructure-including the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries-increasingly is being targeted for exploitation and potentially for disruption or destruction, by a growing array of state and non-state adversaries. Over the past year, cyber exploitation activity has grown more sophisticated, more targeted, and more serious. The Intelligence Community expects these trends to continue in the coming year."*

A Presidential Cyber Security Promise That Could Not Be Kept Because of FISMA

In February of 2000, in the aftermath of the Mafia Boy attacks on Amazon, CNN, Yahoo, and Dell, the President of the United States promised twenty Internet leaders that the US government would "lead by example" in building defenses that would block the growing scourge of cyber crime. But neither the Clinton Administration nor the Bush Administration have led by example, in large part because they were hamstrung by an error in a law called GISRA, the Government Information Security Reform Act. GISRA later morphed into FISMA, but the FISMA drafters did not know of the error, and did not fix it. Because of that error in GISRA, not only are government systems far less secure than they could be, but more than a $300 million dollars of scarce federal security money was spent on writing reports that were never read, and that did not improve security.

How do we know this? Because SANS trains more than 14,000 cyber security professionals each year – with more than 15% employed in federal information security. Our alumni in the working for the federal government and for contractors, like other alumni around the world, keep us up to date on what works and what doesn't in cyber security.

SANS also operates the Internet Storm Center, an early warning system, so we have a pretty clear picture of the threat landscape as well as the effectiveness of the defenses.

Major Federal Successes in Cyber Security Illuminate How FISMA Can Be Improved

On December 10, 2007, SANS published a compendium of federal successes in information security, entitled "What Works in Implementing the US National Strategy to Secure Cyberspace: Case Studies of Success in the War on Cybercrime and Cyber Espionage." I have attached that document for your reference.

A quick review of the federal successes listed in the "What Works" document shows that most were accomplished without any FISMA support or relevance, but that the most important one (the Federal Desktop Core Configuration or FDCC) was enabled by a clause in FISMA [3544(b)(2)(D)(iii)].

That one powerful clause worked because it showed agencies how to prioritize their cyber security actions. It did that by providing direct, unequivocal guidance.

What Went Wrong Because of FISMA

The error in GISRA and later in FISMA was the lack of priority setting. It is best illuminated by showing exactly what went wrong when agencies tried to implement FISMA.

First, the National Institutes of Standards and Technologies (NIST), following its FISMA mandate, wrote a series of guidance documents, later made mandatory by OMB, telling agencies how to comply with FISMA. NIST failed to prioritize the actions it required agencies to take. Instead NIST wrote guidance at a very high level – leaving interpretation to the agencies and their Inspector Generals (IGs). The lack of priorities, along with language open to broad interpretation, made it nearly impossible for agencies to do all the things their IGs might consider as required. None of the agencies had sufficient budgets to do everything, so they did what they could and received Ds and Fs on their report cards because the IGs found that they hadn't done everything.

Far worse than bad grades, however, was the three hundred million dollars wasted in the name of GISRA and then FISMA compliance. That money could have gone a long way toward improving the security of federal systems.

The money was wasted because both Congress and OMB forced agencies (through the annual Congressional Report Card and the President's Management Agenda) to write Certification and Accreditation (C&A)reports on 100% of their systems, using C&A requirements documented by NIST. Every agency had to prepare reports on every system every three years with annual reviews of those systems every year. That would be a wonderful way to monitor improvements in security if the security actions being reported are the essential ones that actually block attacks and improve response to attacks. But guidance from NIST was far too high level. Most of the NIST-specified security measures are disconnected from the key protections. And because the report writers felt obliged to cover all the NIST controls, the reports became essentially useless. Most were never read by the operational staff who would have to implement key security controls. We know that the reports were never read from complaints received from dozens of people frustrated by the process, but the most telling data comes from a meeting of the Northern Virginia Information System Security Association, the membership group of cyber security managers and consultants. While addressing an audience of 72 security professionals there, I asked them to raise their hands if their job involved drafting C&A reports. Fifty-five raised their hands. Then I asked them to keep their hands up if anyone had ever read their reports besides the people who wrote them. Only four kept their hands up.

In other words,

1. FISMA became a report writing exercise caused by
2. NIST language that focused on 'everything' and
3. 'a single scorecard/report card' that indicated 'compliance' to everything (and nothing) and
4. gave a 'false sense' that systems were actually secure -- as demonstrated by the continued infiltrations and exfiltrations.
5. In this case, compliance often had little to do with actual security but Agencies spent all the money on compliance. Why? Because...
6. Leaders are smart. They want to keep their jobs. Congress and OMB (and the press) focused so exclusively on the report cards that CIOs simply spent the money to get Congress and OMB off their backs.

Proof That Tighter FISMA Language Improves Security

One exception demonstrates how to correct the problem. Subsection 3544(b)(2)(D)(iii) of Title 44 tells agencies to establish, implement minimum security configurations for every system. The Air Force demonstrated that following this Congressional rule to the letter enabled it to reduce vulnerabilities significantly, to cut patching time from seven weeks to 3 days and to save tens of millions of dollars. It improved security while reducing costs.

The single most important correction needed in FISMA is to include language that directs NIST to prioritize the actions it tells agencies to take and the frequency for ensuring each action is taken: NIST

guidance would provide specific actions and specific time frames for executing those actions. The most critical actions are to be performed quite frequently. For example:

- Actions performed continuously would include such things as stopping malicious packets from entering the network and alerting security teams when any unauthorized system or service is added to the network.
- Actions performed weekly would include things such as ensuring every system is configured in accordance with the agency's standard secure configuration, and
- Actions that could be performed annually would include such things as security awareness testing.

FISMA can be an important part of the successful defense of the computers and networks that run our government. But to do that it needs to direct agencies to spend their security money on the defenses that make a difference in their ability to protect the information they keep. You can make FISMA do that. At the request of your staffers, we have provided draft changes and report language that we think would help make FISMA more effective.

I would be happy to answer your questions.

About Alan Paller

Alan Paller is director of research for the SANS Institute.

SANS is the primary training organization for the technologists who battle every day to protect the computer systems and networks in the global infrastructure. SANS alumni, more than 68,000 in all, are the security managers, security auditors, firewall analysts, intrusion detection analysts, system and network administrators, incident handlers, forensic analysts, and law enforcement officers who are responsible for building, maintaining, and auditing their organizations' cyber defenses, fending off attackers, and, when attackers succeed, investigating the crime and tracking down the criminals. SANS is also a licensed graduate degree granting institution and an ANSI-accredited security skills certification body. SANS also is a source of situational awareness and continuing education to these technologists on the front-line of protecting our critical infrastructure. Every day, all day and night, analysts at SANS Internet Storm Center receive reports of new attacks and anomalies, analyze those attacks, cross reference them related information and publish daily diaries of the newest attacks being seen. Internet Storm Center also processes information from sensors monitoring 500,000 Internet-connected systems around the world. Each week, more than two hundred thousand individuals and organizations receive SANS NewsBites and @RISK to keep them up to date on new developments in information security and new vulnerabilities and threats.

One of Alan's most important roles at SANS is identifying the most promising security practices and shining a bright light on them so they can be used by other organizations to improve cyber security. His work has been recognized by the Federal CIO Council that named him the Azimuth Award winner in 2005 and by President Clinton who named him as one of the first members of the President's National Infrastructure Assurance Council. Before helping to create the SANS Institute, Alan was an entrepreneur who, with four others, created the first large-scale computer graphics company, took it public, and merged it into a New York Stock Exchange company. Alan's degrees are from Cornell University and the Massachusetts Institute of Technology.

Federal Funding:
Federal agencies send security people to SANS for training and pay tuition for them.

What Works in Implementing the US *National Strategy to Secure Cyberspace*
Case Studies of Success in the War on Cybercrime and Cyber Espionage
A SANS Consensus[i] Document
December 10, 2007

As the ***US National Strategy to Secure Cyberspace*** approaches its fifth anniversary, prudence dictates that the nation measure what has been accomplished under that strategy to determine which efforts should be continued and enhanced, and which need to be altered or discarded.

The successes of the projects described in this paper for securing the nation's cyber infrastructure are worthy of our praise. In fact, they are critical to national security and should be adopted more broadly. However, as we acknowledge these successes, its also essential to acknowledge that the level and sophistication of cyber threats are increasing Organized crime groups in Eastern Europe and Asia are spending hundreds of millions of dollars each year to buy exploits and recruit and employ the best hackers in the world; they are leading a $10 billion financial crime spree. Terrorists are using money stolen from US banks, through cyber fraud, to pay for the bombs that kill innocent people around the world. Certain rogue nation states have concluded that their very survival depends on their ability to penetrate and corrupt US government computers, and they have been enormously successful in infiltrating computers at the Department of Defense (DoD), military contractors, Department of Energy (DoE) labs, the State and Commerce Departments and more. Even the Department of Homeland Security's (DHS's) own computers are not immune and have suffered breaches in their environment.

Clearly much more needs to be done to slow the tidal wave of cybercrime. We hope that the successes illuminated here will serve as prototypes to demonstrate that government leadership by example is both possible and effective.

Measures of Success

Projects were selected for inclusion only after determining that there is evidence of substantial and measurable improvement in the US capacity to meet one or more of the three strategic objectives that shape the ***National Strategy to Secure Cyberspace:***

1. Prevent cyber attacks against America's critical infrastructures;
2. Reduce national vulnerability to cyber attacks; and
3. Minimize damage and recovery time from cyber attacks that do occur.

The evidence of each project's impact needed to be direct, substantial, and measurable since any other criteria would result in the inclusion of an enormous number of ineffective initiatives, most of which have also been very expensive. For example, the Department of Homeland Security's Cyber Storm I national exercise in 2006 might be considered by some to have been a success. It was not included in this list because no substantial, measurable change in behavior or effect can be attributed to it. We may have learned some lessons from the exercise, but there is no substantial evidence to indicate an intent to act on those lessons. On the other hand, the deployment of DoD's Common Access Card (CAC) resulted in a large decrease in the opportunity for unauthorized access to government computers. Similarly, the National SCADA

(Supervisory Control and Data Acquisition) Test Bed and the Control Systems Security Program have already substantially and measurably improved the security of systems that control much of the nation's most critical infrastructures.

In the policy arena, substantial advances have been made, ranging from the ratification of the Council of Europe Cybercrime Convention, to the appointment in DHS of an Assistant Secretary with primary responsibility in cyber security, to the addition of a cyber security sidebar to the Homeland Security Strategy. These advances help shape the landscape of cyber security, but it is nearly impossible to show that they have resulted in significant improvement in any of the three strategic objectives of the *National Strategy*.

For each successful initiative, we describe 1) the challenge it met; 2) the organizations that acted to make it happen; 3) what they did and how they did it; 4) how we know it worked and; 5) an estimate of procurement and operating costs.

1. THE CHALLENGE: Decrease the security vulnerabilities of millions of federal computers while reducing procurement and operating costs.

Federal government agencies spend tens of millions of dollars trying to configure their computers safely and then hundreds of millions more testing and deploying system and security patches as they become available. Even with spending in the multiple millions of dollars, most federal computers do not have consistently secure configurations and most federal agencies take weeks or months to patch their systems. This allows fast-moving cyber attackers the ability to exploit the vulnerabilities before the patches are installed. An analysis by NSA, published in 2002, found that as many as 90% of all vulnerabilities are eliminated through up-to-date patching and secure configuration.

Who: The U.S. Air Force (USAF), National Security Agency (NSA), Defense Information Systems Agency (DISA), National Institute of Standards and Technologies (NIST), DHS, and the Office of Management and Budget (OMB), plus the Center for Internet Security (CIS), Microsoft, and Dell.

What: A standard desktop operating system configuration with integrated security, deployed on over 450,000 computers.

The most important success in federal government cyber security to date is the Federal Desktop Core Configuration (FDCC) and its predecessor proof-of-concept project in the U.S. Air Force. The Air Force, with the help of NSA, NIST and DISA, created a standard configuration of two popular Windows operating systems and then used its procurement power to ensure all relevant computer suppliers delivered computers with the secure configuration installed at the time of delivery. The result was radically reduced costs for implementing security because the standard security configurations were built-in by the vendors. Additional savings were experienced in patch testing and user support since the resources required for these operational activities were significantly reduced. The Air Force proved that procurement, using well-vetted standard configurations, can improve the overall security posture while lowering procurement and operating costs. The Air Force also tested the hypothesis that implementing secure

configurations would cause software applications to break. What they learned was that only a few legacy applications were impacted and then only if those applications required users to run the applications with elevated privileges (a particularly dangerous practice because it puts the system at increased risk of being compromised by remote cyber-attackers).

How effective is this initiative in the U.S. Air Force? Lieutenant General Michael Peterson, Chief of Warfighting Integration and USAF CIO, told *Military Information Technology* magazine, "[the initiative is] reducing our network patch time from 57 days to less than 72 hours while simultaneously cutting the workload for system administrators in half. Ultimately this reduces the cost of software licensing by over $100 million across the FYDP". And of course, faster system patching makes it more difficult for hackers to breach critical systems, resulting in lower costs AND improved cyber security.

The Office of Management and Budget (OMB) actively followed the Air Force experiment from the beginning. When the Air Force project proved successful, OMB leadership issued instructions for all federal agencies to standardize on the secure Air Force configuration as adjusted by NIST. OMB also proactively resolved potential application incompatibility problems by issuing a mandate that no software can be purchased that: 1) doesn't run on the secure operating system configuration or: 2) requires elevated privileges.

The result: Federal agencies gain improved security configurations, faster system patching and lowered procurement and operating costs. Active leadership in the federal government made it viable for Microsoft to create configurations of Windows that are much more secure than standard Microsoft operating system configurations, ultimately, as Microsoft makes the same secure configurations generally available, enabling buyers throughout the world to gain the same benefits of improved security and lower costs.

This project also illustrates how the public-private partnership can work. First, the National Security Agency and the Center for Internet Security (a public-private partnership composed of more than 100 private companies and US and international government members) developed a consensus draft secure configuration for Windows and other operating systems and applications. The Windows configurations were honed by the USAF, Microsoft, NIST, DISA and NSA to become the Federal Desktop Core Configuration (FDCC). Once the configuration was tested and validated, Microsoft, Dell and other PC vendors contracted with the government to deliver the securely configured versions of Windows operating systems. Prior to the creation of the FDCC, these vendors actually wanted to deliver more secure systems but it was too difficult and expensive when every enterprise had its own definition of the 'right' configuration. This project made it possible for system vendors to meet their business objectives AND deliver systems that actually improved security.

Lesson Learned: In procurement, scale means leverage. The combined software budget of the Air Force was substantial. Microsoft and Dell were able to deliver the common configuration easily because the cost of development and deployment could be spread over hundreds of thousands of copies of the software. The combined budgets provided leverage with the appropriate incentives for them to further reduce costs for baking security into the systems they deliver to government and industry.

How much did it cost? Developing the benchmark configurations cost approximately $2.4 million, and initial testing of the new configurations at the USAF cost another $500,000 but the implementation of those configurations actually saved money. The Air Force saved $100 million in software procurement costs by consolidating its procurement across 38 legacy contracts. Additional tens of millions of dollars are being saved in reduced system administration and help-desk costs every year.

2. THE CHALLENGE: Identifying cyber attacks on federal agencies and illuminating federal systems that have been corrupted by cyber attackers. This is especially important in an age of botnets where increasing numbers of federal systems are infected through spear phishing and then used to attack other organizations or to steal sensitive information.

Who: The National Cyber Security Division of the US Department of Homeland Security, National Security Agency, Office of Management and Budget , CERT/CC at Carnegie Mellon University, and several cabinet-level agencies.

What: The Einstein program: enables full-time monitoring and analysis of network traffic received and sent by federal agencies resulting in identification of patterns that may be signs of persistent presence of unauthorized software and users on federal networks. Its expansion into the Trusted Internet Connection (TIC) program extends these benefits to all federal agencies.

Fourteen federal agencies have already deployed Einstein sensors at their network gateways to capture information about network traffic and feed it to analysis programs run by CERT/CC at Carnegie Mellon University in Pittsburgh on behalf of the US Department of Homeland Security. In a dramatic demonstration of the promise of the deployment, network traffic transmitted by the Department of Agriculture and received by the Einstein sensors at the Department of Transportation contained malicious packets that indicated Agriculture systems had been penetrated and infected. The Einstein analysts quickly contacted Agriculture and helped that agency find and eliminate the infection. This is just one of numerous similar examples of Einstein's ability to find infected systems inside agencies.

Under the new Trusted Internet Connection program, federal agencies will reduce the number of Internet connections and ensure all traffic is monitored through the Einstein analytical systems.

How much did it cost? Einstein cost $33 million over the past three years and an additional $14 million per year. TIC will cost hundreds of millions.

3. THE CHALLENGE: Improving the security of industrial control systems at nuclear power plants, utilities and other critical infrastructure elements in both the government and private sectors.

Supervisory Control and Data Acquisition (SCADA) and other control systems often last 20 to 30 years, and most industrial control systems were designed and installed before cyber security threats were known or widely understood. Utilities have now come under

direct attack and some facilities have even been subject to extortion demands by hackers who have broken through the defenses. Thousands of public and private sector organizations need to move quickly toward improving the security of these critical systems.

Who: The Department of Energy; Department of Homeland Security; the State of New York, the Idaho National Laboratory (INL), Sandia National Laboratory (SNL), and Pacific Northwest National Laboratory (PNNL), plus a consortium of control system vendors.

What: The National SCADA Test Bed and the Control Systems Security Program and the SCADA Security Procurement Specifications.

Government Accountability Office (GAO) reports in March 2004 (http://www.gao.gov/new.items/d04354.pdf) and September 2007 (http://www.gao.gov/new.items/d071036.pdf) document "increasing risks due to cyber threats, system vulnerabilities, and the serious potential impact of attacks" against the control systems that manage power plants, electric distribution systems, oil and gas pipelines, water systems, transportation systems, and dams. Reliance on technologies from the 1960s and 1970s, combined with increasing use of newer Windows operating systems and insecure direct and wireless connections of control systems to external networks, have led to substantial vulnerabilities within the nation's critical industries.

The most important success in building a public-private partnership to improve cyber security has been the national effort to secure control systems. The National SCADA Test Bed team assembled a representative group of control systems from most major suppliers and performed in-depth vulnerability tests on those systems. Their testing was sophisticated and comprehensive and the vulnerabilities they found were both important and common across vendor systems. When the Test Bed team finds significant vulnerabilities, INL engineers demonstrate the problem to the system manufacturer. These manufacturers then correct the problem when possible and INL engineers verify that the vulnerability has been eliminated. The vendors are then able to deliver the corrected system to each new customer and sometimes fix the vulnerability in existing systems. Federal funds were significantly augmented with funding from manufacturers and asset owners who wanted to support the Test Bed and ensure testing went beyond those funded by federal agencies.

Vulnerabilities discovered by the testers need to be corrected in all control systems. DHS and DoE funded INL to develop and distribute procurement specifications that utilities in the US and around the world are already using to ensure their control system vendors are delivering baked-in security. With the assistance of the Multi-State Information Sharing and Analysis Center, led by New York State, and the United Kingdom's Centre for the Protection of the Critical National Infrastructure (CPNI), these specifications are being adopted in the US and are being considered for formal adoption by a ten-country consortium.

The result: Many vulnerabilities in control systems have been found and corrected, and, using the new procurement specifications, buyers of SCADA and control systems can tell vendors exactly what is needed and ensure important vulnerabilities are eliminated.

How much did it cost? The National SCADA Test Bed and Control Systems Security Program cost approximately $17 million annually in federal funds over the past four years (funds that have been cut back sharply in the current year) and more than $4 million in private funding (contributions of equipment for testing, for example) by control system vendors and utilities in support of testing and where industry needed additional testing not funded by the federal programs.

4. THE CHALLENGE: Raising international barriers and increasing criminal penalties for cybercrime by identifying and capturing more cyber criminals and incarcerating them for longer periods.

Cyber criminals live and work in many countries. When one of those countries has weak laws against hacking or when that country's law enforcement organizations have neither the skills nor the will to pursue hackers attacking foreign systems, the criminals know they can operate with impunity. Even where cybercrime is illegal, sentences for convicted cyber hackers were very lenient -- often simply probation.

Who: The Justice Department's Computer Crime and Intellectual Property Section (CCIPS), the FBI's Cyber Security Program, and the cyber security programs of the US Secret Service and the US Postal Inspection Service.

What: 1) Bilateral and multi-lateral agreements between law enforcement groups in the US and other countries allowing immediate capture of cyber criminals through real-time cooperation; 2) Better education of prosecutors, investigators and judges about how to investigate and prosecute cybercrime cases and the damage to businesses and other organizations caused by cybercrime; 3) Improved law enforcement techniques and tools to identify and capture more criminals and; 4) the National Cyber-Forensics and Training Alliance (NCFTA).

The US Department of Justice's Computer Crime and Intellectual Property Section (CCIPS) has attempted to standardize cybercrime law internationally through the development and support of the Council of Europe's Convention on Cybercrime. CCIPS used active diplomacy to provide technical assistance to countries around the world to help them synchronize their cybercrime laws, and, with the help of federal investigative agencies, helped them build much stronger cyber law enforcement capabilities. In addition, by developing and maintaining the G8 Hi-Tech Crime Subgroup's 24/7 Points of Contact Network involving 50 nations, CCIPS facilitated a means of expediting requests for, and responses to, international needs for assistance in urgent cybercrime matters. CCIPS also created the Computer Hacking and Intellectual Property (CHIP) Network of approximately 230 Assistant United States Attorneys (AUSAs) around the country. The CHIP Network coordinates investigations and provides training, knowledge, and assistance on the prosecutions of computer and intellectual property crimes to AUSAs in United States Attorneys' offices throughout the country.

At the same time, the FBI built cyber squads in dozens of field offices and established legal attaché offices ("legats") in 60 countries around the world. Those squads and international law enforcement partners supported by the legats have had impressive success in finding and capturing cyber criminals. In parallel with these efforts, the FBI has put a dozen full-time cyber

investigators into a facility that also houses representatives of universities and more than a dozen leading US corporations. The public-private initiative, called The National Cyber-Forensics and Training Alliance (NCFTA), has accounted for the identification of more than 1,900 phishing drop sites (where the victims' data are stored), resulting in the prevention of tens of millions of dollars in losses. NCFTAs' work also led to the recent arrest of several dozen people involved in international credit card fraud enabled by cyber-theft of private information.

The US Secret Service and the US Postal Inspection Service also played huge roles in many major, successful cyber investigations and are pillars of the national initiative to make cyber criminals pay for their crimes.

The result: Law enforcement officials have had many more successful investigations and prosecutions of cyber criminals, and judges have been meting out much longer sentences – six years or more in some recent trials. That's up from less than a year just five years ago. All of this has helped send a good deterrent message that is essential to securing cyberspace.

How much did it cost? Because almost every major crime today has a cyber dimension and nearly all cybercrime has an international dimension, it's impossible to calculate the cost of this important initiative. The NCFTA costs $1.5 million per year (in addition to the salaries of the federal investigators).

5. THE CHALLENGE: Making remote exploits of federal computers more difficult by ensuring that only authorized users gain access. User names and passwords are insufficient to ensure that only authorized people are using computers.

Who: Department of Defense (DoD), GSA, OMB and most federal civilian agencies.

What: Implementing two-factor authentication for all personnel requiring access to government computer systems.

The US Department of Defense distributed Common Access Cards (CAC) enabling the DoD to ask every would-be user of its networks and computer systems to have a card in his or her possession and to know a personal identification number or password. Requiring two different forms of identification – one the user has in his or her physical possession and one the user knows, is called two-factor authentication. Two-factor authentication is a proven method for decreasing intrusions and other types of security breaches by ensuring that stolen user names and passwords are insufficient to gain access to networks.

DoD's success with its Common Access Card led the US Office of Management and Budget to issue Homeland Security Presidential Directive 12 (HSPD-12), requiring all federal agencies to implement two-factor authentication. As agencies fully implement HSPD-12, they will gain the same benefits that DoD has obtained.

The result: On January 25, 2007, Lt. General Charles Croom, USAF, told an audience in Colorado Springs, "Although there are six million probes of Defense Department networks a

day, successful intrusions have declined 46 percent in the past year because of a requirement that all DoD personnel log on to unclassified networks using Common Access Cards."

Large-scale procurement of Common Access Cards by DoD and emerging procurements by other federal agencies under HSPD 12 has already reduced the cost of deployment from over $100 to less than $50 per card.

How much did it cost? The DoD Common Access Card program cost more than $6 million just for the R&D process and then tens of millions more for deployment. HSPD-12 implementation to date has cost in excess of $100 million.

6. THE CHALLENGE: Safeguarding sensitive data stored on mobile (laptop) computers from loss or theft.

Tens of thousands of government computers have been lost or stolen and the data on many of those systems were unprotected and unencrypted. The embarrassment to federal agencies has been acute and senior officials have been consumed by responding to Congressional inquiries and press questions.

Who: DoD, GSA, Office of Management and Budget, and the Multi-State Information Sharing and Analysis Center.

What: SmartBuy provided federal government agencies with a low-cost acquisition vehicle for laptop encryption software and extends the benefits of that procurement to state and local governments.

Encrypting the data on mobile devices (laptop computers, PDAs and cell phones) makes sense but encryption software and hardware are expensive. Consequently, most organizations have been unable to commit to widespread implementation. The economics of software offers an easy solution but it requires a catalyst to make it happen. The cost of making each additional copy of a software package is very low, so if a software vendor is assured of selling vast numbers of additional copies, that vendor can lower the price and still earn potentially greater profits. One buyer has to be first to prove that the number of copies to be sold is very large. In this project, the Federal SmartBuy program proved to software vendors that they can lower prices substantially when volumes are large enough.

The result: Under the old GSA contract, federal agencies could buy, for example, SafeBoot, a popular full-disk laptop encryption product, for $99 per copy in quantities under 100. When an agency buys 5,000 to 10,000 copies, the price is $81.99 per copy. Most agencies that buy more copies have been able to push the prices down to between $55 and $60 per copy. But in September 2007, under the new large-volume SmartBuy initiative, the Department of Agriculture bought 180,000 copies of encryption software for $1.8 million or $10 per copy. In other words, consolidated federal buying power guaranteed sufficient quantities that enabled the software vendor to provide discounts of nearly 90%, and still earn a healthy profit. This example of federal procurement leadership is especially important because the US government contracting initiative enabled state and local governments to also buy software under the new

contract. This allowed fiscally strapped small government organizations to buy five to ten times as many copies of encryption software for the same price they would have had to pay without federal procurement leadership.

How much did it cost? The effort to create the SmartBuy contract cost about $300,000 but the resulting savings are huge. Just at the Department of Agriculture, the direct savings exceeded $7 million.

The Most Promising Federal Cyber Security Program on the Horizon

THE CHALLENGE: Improving the ability of agencies to keep their systems patched in the face of a flood of new vulnerabilities that exceeds human capacity to find and fix before systems are exploited.

Who: The National Security Agency (NSA) and the National Institutes for Standards and Technology (NIST), Microsoft and other commercial system and security software vendors.

What:, The Security Content Automation Program (S-CAP) will make it possible to automate the entire chain of events from vendors reporting vulnerabilities and how to find them, to vulnerability testers finding the flaws, to system mangers and configuration software programs recording the full state of each system, ultimately to patching tools actually correcting the problems, all in real time, without human intervention.

This is one of the most promising projects in cyber security because it engages all the players, from application and system software developers to system management tool suppliers to security tool suppliers, to upgrade their tools so they can work together to protect federal and other critical systems. It promises to radically lower the cost of maintaining security "hygiene" and promises a future in which security professionals focus on other problems.

How much did it cost? Approximately $12 million to date but the amount will grow substantially when commercial organizations re-engineer their processes and software to use the automated protocols. On the other hand, once S-CAP is fully operational, agencies and industry can expect substantial cost reductions because they will be able to eliminate much of the manual effort currently associated with finding and fixing vulnerabilities in the software they have deployed.

Why is it promising and not yet a full success? S-CAP has not yet been implemented in enough commercial tools to enable full automation.

---

[1] The authors of this document are Alan Paller of the SANS Institute, Paul Kurtz of Goodharbor, Jim Lewis of the Center for Strategic and International Studies, John Gilligan of SRA, and Frank Reeder. Others who provided valuable input include Will Pelgrin of New York State, Christopher Painter of the US Department of Justice, Marjorie Blumenthal of Georgetown University, Mark Weatherford of the State of Colorado, Clint Kreitner of the

Center for Internet Security, Marcus Sachs of Verizon, Eugene Schultz of High Tower, and Mason Brown, Johannes Ullrich, Stephen Northcutt and Eric Cole of the SANS Institute.

Mr. CLAY. Thank you so much for that enlightening report.
Mr. McConnell.

STATEMENT OF BRUCE W. MCCONNELL

Mr. MCCONNELL. Thank you, Mr. Chairman and members of the subcommittees for the privilege and opportunity to testify today on Federal information security.

The jurisdiction of this committee is so broad and its work is so important to the critical functioning of our Federal Government, it is a real pleasure.

I am here today bringing you the perspective of 20 years of work in information policy and technology, including 15 years at OMB, serving 3 Presidents. I am also on a commission for cyber security for the 44th Presidency, which has been co-chaired by Congressman Jim Langevin and Congressman Michael McCaul. I am not speaking on behalf of that commission.

You asked in your invitation that I provide policy recommendations for potential legislative consideration and to comment on the state of FISMA compliance and the provisions of H.R. 4791. I have done that in my written statement.

But in my oral remarks, I wish to focus in on what I consider to be the most significant development in Federal information security in many years. My analysis is based solely on information that is in the public domain.

On January 8th, President Bush issued a new National Security Homeland Security directive. This order establishes a comprehensive national cyber-security initiative. The issuance of this national security order shows that information security is receiving serious attention at the highest levels of the executive branch. I believe this is good news.

The so-called Cyber Initiative recognizes the serious threats to the Nation's information infrastructure coming from State and non-State actors, including sophisticated criminals. It lays out the need to take proactive measures in cyberspace to detect and prevent intrusions from whatever source in real time before they can do significant damage. These tenets are important, and while the details are not yet public, they clearly include an increased role for the intelligence community, in particular the National Security Agency [NSA], in protecting Federal systems.

Let me explain why I believe this expanded NSA role is germane to this committee's work. The Cyber Initiative relates directly to two statutes under your jurisdiction: FISMA and the Privacy Act. When this committee wrote FISMA's predecessor, the Computer Security Act of 1987, you vested the National Institute of Standards and Technology [NIST], with primary authority in the security of civilian agency information systems. You also explicitly limited the role of NSA with respect to civilian agency systems. There were several reasons for this differentiation of responsibilities.

Foremost in the mind of Congress was the potential chilling effect on the free flow of information between Government and the public, including the information technology industry, if a military agency became too closely involved with civilian agency systems. As the committee's report in 1987 notes, "Since it is a natural tendency of DOD to restrict access to information through the classifica-

tion process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information."

Civilian agency missions, such as those at the Census Bureau, the Internal Revenue Service and the Centers for Medicare and Medicaid Services, depend on the trust of the American people to operate successfully. These missions require the free and efficient flow of information to and from the public in order to deliver important public benefits and programs.

In addition to the potential chilling effect on information flows, the statute also reflected potential concerns about privacy and civil liberties. This statutory framework separating civilian and military systems has been confirmed and strengthened three times in the last two decades.

Now, Mr. Chairman, it may be that the world has changed so much that this historic distinction between civilian agency systems and national security systems no longer serves the Nation's interest. Certainly the current computer security regime in Government is not working adequately. There is a big gap between what the agencies need and what they are getting. The gap extends beyond Government systems to the U.S. information infrastructure.

Therefore, there is a substantial argument that you need to put resources from the intelligence community against this problem, because that is where the most resources are on the Federal side. Of course, there is also substantial resources in the private sector in this area.

So what is really needed is a partnership of trust between the Government and the private sector to address the Nation's information security needs. Many of the information security professionals I talk to suggest that this trust is at a relatively low point in our history and it needs to be strengthened if we are going to be able to address this critical issue. We need to determine who in the Government can most effectively foster trust and cooperation with industry and with the American people.

So I encourage the committee to look at these roles and responsibilities in the context of FISMA and the Privacy Act. Thank you, sir.

[The prepared statement of Mr. McConnell follows:]

McConnell
INTERNATIONAL

Written Statement of

Bruce W. McConnell

President
McConnell International, LLC
www.mcconnellinternational.com

before the
Subcommittee on Information Policy, Census, and National Archives
and the Subcommittee on Government Management, Organization, and Procurement
of the Committee on Oversight and Government Reform
U.S. House of Representatives

Federal IT Security: A Review of H.R. 4791

Thursday, February 14, 2008

Thank you, Mr. Chairman and Members of the Subcommittees, for the privilege and opportunity to testify today on the critical topic of federal information security. The jurisdiction of this Committee is wonderfully broad, and its work is so critical to the effective functioning of our federal government.

My name is Bruce McConnell, and I served in the Office of Management and Budget from 1985-2000, under three Presidents. During that time I was the Chief of Information Policy and Technology, which was the most senior position at OMB concerned primarily about federal information technology matters, and in particular, IT security. In that role I had the opportunity to work with this Committee on many occasions, most notably in the development and passage of the Computer Security Act of 1987, the Clinger-Cohen Act, and several iterations of Paperwork Reduction Act. I also had the responsibility to oversee the implementation of these statutes in the federal agencies, and to develop policies to assist the agencies in performing their missions with the support of IT.

Since 2000, I have been president of a small, eponymous consulting company that works with government and industry to find private sector solutions to pressing federal mission support requirements. I am presently a member of the Commission on Cybersecurity for the 44th Presidency, which is co-chaired by Congressman Jim Langevin and Congressman Michael McCaul, and has been convened by the Center for Strategic and International Studies.

Finally I should mention that, while I was at OMB, I co-chaired the Interagency Working Group on Encryption Policy. Made up of representatives of the intelligence community, the State, Defense, Justice, and Commerce Departments, this group was responsible for reforming U.S. export control policy to enable the use of strong American-built encryption on the global information infrastructure, increasing the security of information that resides there.

You have asked that I provide you with policy recommendations for potential legislative consideration, and to comment on the state of the Federal Information Security Management Act (FISMA) compliance government wide and the provisions of H.R. 4791.

Policy Recommendations

The Nation finds itself at a momentous time. We are ever more dependent on information systems for our livelihood and survival, yet we are falling behind in terms of keeping the systems, both public and private, secure in the face of increasingly sophisticated threats. As a result there is growing attention to the importance of information security. This welcome increase in awareness can be seen on numerous fronts.

- This Committee continues to step up its leadership efforts.
- The Administration has requested a marked increase in funding, and has underway several initiatives, including the Information Systems Security Line of Business, the Trusted Internet Connection program, the Federal Desktop Core Configuration program, the Common Identification Standard for federal computer access, and the Einstein monitoring program.[1]
- A vast number of efforts are underway in the private sector, including the excellent work of the SANS Institute and the CSIS Commission.
- And, on February 5, 2008, the Director of National Intelligence, J. Michael McConnell, provided the outlines of what is known as the "Cyber Initiative."

I want to begin my discussion of policy by examining the Cyber Initiative, because it is the most significant development in the federal information security arena in many years. My discussion is based on the DNI's testimony, and on statements by OMB officials in a public briefing on the IT budget last week. My analysis is somewhat limited, as the details of the Initiative remain classified for national security reasons.

The Cyber Initiative

On January 8, 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. This order establishes a comprehensive, national cybersecurity initiative. The issuance of this order shows that information security is receiving attention at the highest levels of the federal

[1] *See*, variously: Fiscal Year 2009 IT Budget Rollout Presentation, Proposed IT Security Spending, http://www.whitehouse.gov/omb/egov/documents/FY09_IT_Budget_Rollout.pdf, pages 3-4; Budget of the United States Government, Fiscal Year 2009, Table 9-9, "Lines of Business Update," http://www.whitehouse.gov/omb/budget/fy2009/pdf/ap_cd_rom/9_9.pdf; "Implementation of Trusted Internet Connections," OMB Memorandum M-08-05, November 20, 2007, and, "Planning Guidance for Trusted Internet Connections," undated memorandum to chief information officers from Karen S. Evans; "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," OMB Mamorandum M-07-11, March 22, 2007; Homeland Security Presidential Directive (HSPD) 12, "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; Budget of the United States Government, Fiscal Year 2009, Analytical Perspectives, Homeland Security Funding Analysis, page 27.

government, a most timely occurrence. In addition, its issuance as a national security order shows an additional seriousness of intent. I believe this is good news.

The initiative recognizes the serious threats to the infrastructure by state and non-state adversaries, including sophisticated criminal elements. It lays out the need to deter hostile action in cyber space by making it harder to penetrate our networks. And it makes clear the need to take proactive measures to detect and prevent intrusions from whatever source, as they happen, before they can do significant damage.

These tenets are important, yet they leave many questions unanswered. For example:

Coverage: The initiative clearly includes government systems, both civilian agency systems and national security systems. But how much further does it go towards protecting the national information infrastructure and the critical private sector systems that are part of it?

Activities: Real time monitoring of systems is included, as is preventative response. But how far does the preventative response reach, what does it involve, and how are trade-offs evaluated in terms of potential damage to the national infrastructure from retaliation from the attackers or collateral damage from our own actions?

Roles and responsibilities: There is clearly an increased role for the intelligence community in protecting systems. But how are agencies such as DHS, the FBI, and OMB involved, what procedures are used to authorize specific activities, and who is responsible for oversight?

Authorities: How does the initiative fit into existing statutory frameworks including the Protect America Act, the Foreign Intelligence Surveillance Act, the wiretapping statutes, FISMA, and the Privacy Act?

Let me explain why I believe these questions are important to the Nation, and germane to this Committee's work.

This Committee's Leadership in Ensuring Open Government

This Committee has long been a leader on government information and information security policy. Indeed, no other Committee has paid attention to these matters so consistently and thoroughly over the years.

The Cyber Initiative relates directly to two statutes under this Committee's jurisdiction, FISMA and the Privacy Act. The Initiative deals directly with federal systems security, the domain of FISMA, and it reaches into areas of the Privacy Act because of the personally identifiable information that is collected during the monitoring of federal networks.[2]

---

[2] In addition to these policy points, there are potential operational security impacts of more extensive network monitoring. Recently a group of six renowned computer security professionals wrote about unauthorized breaches in Greek and Italian monitoring systems, noting that surveillance technology is an "architected security breach" that "creates serious security risks: the danger of exploitation of [cont., p.4]

At this moment in our Nation's history, a particularly important area of policy is brought into focus by the Cyber Initiative:

How do we, as a Nation, balance effective security with openness in government?

When this Committee wrote, and the Congress passed, the Computer Security Act of 1987, you gave the Office of Management and Budget policy and general oversight authority for civilian agency systems, vested the National Institute of Standards and Technology (NIST) with authority to issue binding guidance, and entrusted agencies to make decisions about implementing and monitoring their networks – balancing the risk and potential magnitude of harm posed by threats against the need to operate systems critical to achieving the agency's mission. Congress also specified the role of the National Security Agency (NSA) with respect to civilian agency systems – one limited to providing technical assistance to NIST.

There were several reasons for this differentiation of responsibilities.

Foremost in the mind of Congress was the potential chilling effect on the free flow of information between government and the citizenry, including the information technology industry, if a military agency became too closely involved with civilian agency systems. With respect to the effectiveness of the NIST standards program, the Committee's report noted:

> "While the Committee was considering [this Act], proposals were made to modify the bill to give NSA effective control over the computer [security] standards program. * * * This would jeopardize the entire Federal standards program. The development of standards requires interaction with many segments of our society, i.e., government agencies, computer and communications industry, international organizations, etc. [NIST] has performed this kind of activity very well over the last 22 years. NSA, on the other hand, is unfamiliar with it.[3]

Later, on the broader issue of citizen-government information flows, the report observes:

> "Since it is a natural tendency of DOD to restrict access to information through the classification process, it would be almost impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information." [4]

---

the system by unauthorized users, danger of criminal misuse by trusted insiders, and danger of misuse by government agents." Bellovin, Blaze, et.al., "Risking Communications Secuity," IEEE Security and Privacy, 2008, www.computer.org/security.

[3] U.S. Congress, House of Representatives, Committee on Government Operations, *Computer Security Act of 1987—Report to Accompany H.R. 145*, H. Rept. 100-153, Part II, 100th Cong., 1st sess., June 11, 1987 (Washington, DC: U.S. Government Printing Office, 1987), pp 25-26.

[4] Ibid., p. 29.

Indeed, the NSA operates under a different set of norms and authorities than the civilian agencies do. These norms and authorities are properly drawn against foreign and terrorist threats, and support monitoring and response activities against such threats. Likewise, the mission of numerous classified systems properly requires the analysis, identification, and targeting of suspect actors; accordingly, these systems build in many features that limit open access and anonymity.

Conversely, civilian missions, such as those at the Census Bureau, the Internal Revenue Service, and the Centers for Medicare and Medicaid Services, depend on the trust of the American people to operate successfully. The systems that support these missions operate primarily in the domestic environment, where the mission often requires the free and efficient flow of information and open use by the public in order to deliver important public benefits and programs.

Concerns were also raised during the debate on the Computer Security Act about potential risks to privacy and civil liberties if the intelligence community became actively involved in the management of civilian agency systems. In part to address this concern, the Congress established the Computer System Security and Privacy Advisory Board as a senior advisor to OMB, NSA, NIST, and the Secretary of Commerce. Congress emphasized the importance of this concern in 2002 by renaming the Board as the Information Security and Privacy Advisory Board (ISPAB) as part of FISMA.[5]

Thus it was the view of the Congress in 1987 that the importance of maintaining citizen trust in government systems was best served by giving a civilian agency the leadership role.

This statutory framework has been confirmed and strengthened three times in the last two decades – first in the Clinger-Cohen Act of 1996, again in the Government Information Security Reform Act in 2000, and most recently in FISMA. One notable addition to the framework was Section 3544(e) of FISMA, "Public Notice and Comment," which provides that:

> "Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public."

To date, this provision of law has received scant attention from OMB or the agencies, even though it is broadly consistent both in its requirement and its intent with similar provisions in the Paperwork Reduction Act, the Clinger-Cohen Act, and the E-Government Act of 2002.[6]

---

[5] At its most recent two-day meeting in December 2007, the ISPAB reviewed such topics as the role of the Inspectors General, the Einstein program, the state of identity management in the Department of Defense, and status of the National Communications System. *See:* http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2007-12/Dec-2007.html

[6] *See:* Paperwork Reduction Act, Section 3517(a), (44 USC 3510 17(a)); the Clinger-Cohen Act (40 U.S.C. 1131(d)(2)); and Section 207 of the E-Government Act of 2002 (relating to the availability of information to the public via agency websites), subsection (f)(2)(A)(i)).

Has The Policy Outgrown Its Usefulness?

It may be that the world has changed so much that the historic distinction between civilian agency systems and national security systems no longer serves the Nation's interest. Certainly, the current computer security regime in government is not working adequately. While progress is being made, it is happening far too slowly. In a networked world where the system is only as secure as the weakest node, progress is far too uneven. Further, as discussed below, FISMA implementation has proven to be a mixed blessing with respect to computer security. As one computer security professional put it recently, "It was pretty clear last year that 100% FISMA compliance does not bother the Chinese spies."

One of the key weaknesses of the historic distinction has been that the Computer Security Division at NIST, while being entirely well intentioned and staffed by dedicated professionals, has never been positioned or resourced in a way to make it an effective leader in federal computer security. Buried within a research bureau of the Department of Commerce, it is no match—in terms of the depth of its capabilities and influence—for a well-funded, high-tech, operational entity like NSA. As a result, the civilian agencies have received less technical assistance than they need to protect their systems in the current threat environment.

Similarly, the effectiveness of the Department of Homeland Security in this arena has, to date, been a considerable disappointment to most observers. For example, the placement of the policy official responsible for cybersecurity activities was criticized both for its fluidity following the creation of the Department, and for not sitting at a very senior level within the Department; DHS' own cybersecurity performance under FISMA has been consistently graded at F or D; and, recently, a House Homeland Security Committee hearing cited a newly released GAO report that found "pervasive and systemic security problems at the DHS."[7]

Of course, the effectiveness of NSA's information security program is debatable as well. NSA is responsible for "protecting all classified and sensitive information that is stored or sent through U.S. government equipment."[8] Traditionally the agency has focused on Department of Defense systems. However the DOD has not demonstrated itself to be consistently strong on information systems security, at least for the systems that handle unclassified (including sensitive) information.

A gap like this provides an ideal environment for attackers to enter and damage government systems, with potential effects both on those systems and other government systems, including national security systems, which they may communicate with. It also can enable attackers to reach beyond the public information on civilian agency systems, and gain access to such highly sensitive information as

---

[7] Information Security: Homeland Security Needs to Enhance Effectiveness of Its Program, Statement of Gregory C. Wilshushen, Director, Information Security Issues, US Government Accountability Office, GAO-07-1003T, June 20, 2007.

[8] NSA website, "Introduction to the National Security Agency/Central Security Service," http://www.nsa.gov/about/index.cfm, February 12, 2008.

unreleased economic data, taxpayer records, law enforcement information, and health information.

And the gap extends beyond government systems. In the view of Mike McConnell, the Director of National Intelligence:

> The US information infrastructure--including telecommunications and computer networks and systems, and the data that reside on them--is critical to virtually every aspect of modern life. Therefore, threats to our IT infrastructure are an important focus of the Intelligence Community. As government, private sector, and personal activities continue to move to networked operations, as our digital systems add ever more capabilities, as wireless systems become even more ubiquitous, and as the design, manufacture, and service of information technology has moved overseas, our vulnerabilities will continue to grow.[9]

There is, therefore, a substantial argument that national and homeland security of the U.S. require additional resources to be devoted to information security, and further, that the majority of governmental resources for that purpose reside today in the national security community.

Of course, as illustrated by today's panel, there is also substantial private sector capability in this area. Indeed, as is often said, our Nation's critical infrastructures are largely privately owned. What is needed is an effective partnership of trust between the government and private sector to address the Nation's information security needs.

I encourage the Committee to examine this question of roles and responsibilities from a policy standpoint, to determine whether changes in the law are needed. More specifically, the Committee might be interested in exploring the following topics:

1. To the extent that the President's "cyber initiative" gives leadership to the national security community for civilian agency information security, is this change permanent, or is there a transition plan to grow the capabilities of DHS and NIST and return responsibility to them?

2. How will the public be involved in defining security standards and practices of the federal agencies?

3. To the extent that monitoring on government networks involves the collection of information about the public, what safeguards are in place for that data's storage, what minimization procedures are in place to limit such collections, and what governs access to the data that is collected?

4. What procedures are followed to authorize any response activities, and what safeguards are in place to avert "collateral" damage to private sector systems that could occur in retaliation for a response?

5. How does the new policy square with existing statute?

---

[9] Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence, February 5, 2008, p. 16.

State of FISMA Compliance and H.R. 4791

In addition to providing these general policy recommendations, I want to turn now more specifically to the state of FISMA compliance and in particular H.R. 4791.

Mr. Chairman, there are many in the computer security community who believe that FISMA is a mixed blessing. On the plus side, it has had two good macro effects:

- It has increased awareness of the importance of computer security among CIOs and their bosses.
- It has improved the agencies' knowledge of and control over what is connected to their networks and what needs to be managed.

However, in the years since its passage, it has also generated a culture of compliance that often distracts attention from strong operational security measures. In some agencies, more attention is paid to creating a reporting architecture that will increase FISMA scores than to creating a security architecture that will reduce vulnerabilities and minimize the effect of attacks and breaches.

In this context, H.R. 4791 should be looked at from the standpoint of its likely effect on operational security in the federal agencies.

To begin with, Section 7, which changes the currently required "independent evaluation" into a required "independent audit" is potentially problematic and could foster adversarial relationships and not cooperation. This issue was the topic of much discussion during the original development of FISMA. By calling for an evaluation and not a formal audit, the FISMA authors wanted to give to Inspectors General maximum flexibility in assessing their agency's security program, promote cooperation between the IGs and agency officials, encourage resource and information sharing throughout the year, avoid competition for scarce expert security personnel, and insulate agency employees from negative audit "findings" for efforts designed to improve security. I understand that the intent of this provision is to encourage the use of standardized evaluations across all agencies. I believe this could be accomplished within the framework of evaluations, without requiring formal audits. For example, OMB and the IGs could be encouraged to work together to develop such a standardized set of evaluation criteria within a specific time frame.

While the provisions for protecting personally identifiable information (Section 8 and 9) and the risks of peer-to-peer file sharing (Section 6) are important (and have for the most part already been addressed administratively by OMB), they may be too specific and too media/technology dependent to be appropriate for such detailed consideration in statute. The technology environment is changing ever more rapidly, and, in my experience, it is useful to provide the agencies with flexibility to address risks as they deem most appropriate, subject to strong oversight. The inclusion of these detailed provisions could suggest that these risks are the highest priorities that should be addressed in terms of sensitive information. Even if that is true today, it is unlikely to be the case tomorrow.

In addition, while agency relationships with and use of data provided by data brokers is a significant and growing issue, and the definition of Personally Identifiable Information a is a critical question, I am concerned the bill invokes only the limited procedural requirements required by section 208 of the E-Government Act, and not the more fundamental requirements of the Privacy Act. The Privacy Act is of course an important area of this Committee's jurisdiction. That Act forms the principles and program for how the Executive agencies are to acquire, safeguard, use, share, and dispose of personal information pertaining to U.S. citizens. Establishing separate and perhaps incomplete privacy controls and requirements outside the Privacy Act potentially undermines the Act and could create confusion, reducing the effectiveness of the new controls. I encourage the Committee to consider the broader implications of its legislative agenda in this area.

Indeed, given the changes in technology and the world, it may be time to update the Privacy Act of 1974. This major undertaking might usefully be begun by chartering a commission to examine the field and provide recommendations to this Committee.

# # # # #

Mr. CLAY. Thank you so much, Mr. McConnell. Our final witness will be Mr. Bennett. Mr. Bennett, you may proceed.

STATEMENT OF TIM BENNETT

Mr. BENNETT. Thank you, Mr. Chairman, Congressman Davis. Thank you for the opportunity to share the views of the Cyber Security Industry Alliance on improvements in FISMA.

CSIA is a group of leading security technology vendors that are dedicated to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. It is our belief that a comprehensive approach for enhancing the security and resilience of information systems is fundamental to economic security.

Mr. CLAY. Excuse me, Mr. Bennett, is your microphone on?

Mr. BENNETT. Allow me to commend this subcommittee and its parent committee for the sustained attention that has been given in recent years to the critical objective of strengthening information security within the Federal Government. As we have painfully learned and heard from a couple of the other witnesses this morning, Federal systems are frequently vulnerable to cyber attacks, and the oversight of this subcommittee and full committee are an important element in holding Federal agencies accountable for improved information security as well as highlighting ongoing challenges and vulnerabilities.

The 110th Congress now has an important opportunity to amend FISMA to improve the information security climate at our Federal Government agencies. Even though the last few years have yielded a number of successes, there are certain weaknesses in our Government's critical infrastructure which still urgently need to be addressed.

It has become clear that the infiltration of Federal Government networks and the possible theft and/or exploitation of information are among the most critical issues confronting our Federal Government. While progress has been made, much work remains to be done in order to truly secure our Government's IT infrastructure.

FISMA has been fairly successful at getting agencies in general to pay closer attention to their information security obligations. Before FISMA, information security was not a top priority at Federal agencies. FISMA has been successful in raising awareness of information security in the agencies and also in Congress.

However, Federal agencies scored an average grade of C minus in 2007's Information Security Report Card. Some argue that FISMA does not adequate measure information security. A high FISMA grade doesn't mean the agency is secure and vice versa. That is because FISMA grades reflect compliance with mandated processes. They do not measure how much these processes have actually increased information security.

In particular, the selection of information security controls is subjective and not consistent across Federal agencies. Agencies determine on their own what level of risk is acceptable for a given system. They can then implement the corresponding controls, certify and accredit them and thus be compliant and receive a high grade regardless of the level of risk they have deemed acceptable.

Certainly we want to avoid a check the box mentality and don't want FISMA to be reduced to a largely paperwork drill among the departments and agencies, consuming an inordinate amount of resources for reporting progress while yielding few genuine security improvements. Unfortunately, in some cases, that is what it has become.

Some Federal agency chief information security officers are measured on their compliance scores with FISMA, not on whether they have adequately assessed risk in their respective agency or prevented breaches of sensitive information. Instead, we want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. With the benefit of 5 years' experience under FISMA and several insightful reports by the U.S. Government Accountability Office, it is now possible to identify possible improvements that can address those weaknesses in FISMA implementation that have now become apparent.

With global attacks on data networks increasing at an alarming rate and in a more organized and sophisticated manner, there is precious little time to lose. Faced with this urgent need, we applaud the bill that you have introduced, H.R. 4791. We strongly support this bill. It would undertake the important step of codifying many of the recommended steps that OMB took in a series of memos to Federal agencies after a series of significant data breaches in recent years. The legislation provides much-needed common sense obligations to require agencies to develop policies and plans to identify and protect personal information, develop requirements for reporting data breaches and report to Congress a summary of information security breaches reported by Federal agencies.

We recommend that the proposed legislation also include language requiring that data breaches of information systems maintained by contractors and other sources working on Federal projects be promptly notified to the Secretary and the CIO of the contracting agency. Federal contractors are responsible for many of the data breaches that agencies reported. CSIA believes that it is important to reaffirm that FISMA applies to Federal contractors.

We also commend the chairman for having the insight to incorporate language into this legislation requiring that Federal Government agencies encrypt or make unusable and unreadable personal data and to establish minimum requirements for protection of information or mobile devices. H.R. 4791 also prudently establishes security requirements for peer-to-peer networks. We believe that agencies should be required to develop a plan to protect against the risks of peer-to-peer networks and provide detailed technology and the policy procedures they should take.

To assist further consideration of this bill, we offer additional recommendations. One, align responsibilities and authorities to vest the CIO and CISO with specific power over information security. The current authority of agency CIOs to ensure should be the power to enforce cost effective measures of security.

Two, require improvements to assessment, continuous monitoring and remediation in order to develop a comprehensive approach to information systems security. Three, mandate preparation of the

complete inventory of all Federal agency IT assets by a certain date. Four, improvement performance measurement and provide incentives to agencies that give information security a high priority. Five, institutionalize security within Federal agency culture. Six, increase Federal agency IT security funding. Seven, reaffirm objective assessments of commercially available information technologies. And eight, narrow the scope of the privacy definition provided for in the proposed legislation.

In closing, I commend the subcommittee for highlighting the importance of information security, for examining how we can improve FISMA and Federal agency information security practices going forward. The overriding objective should be to move Federal agencies to act in a manner that equates strong information security practices with overall mission accomplishment. We all know what is at stake.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Bennett follows:]

Prepared Testimony of
Tim Bennett
President
Cyber Security Industry Alliance

Before the House Oversight and Government Reform Committee
Subcommittee on Information Policy, Census, and National Archives

Thursday, February 14, 2008
11:30 am
Rayburn Building Room 2154

Chairman Clay, Ranking Member Turner, and other Members of the Subcommittee on Information Policy, Census, and National Archives, I thank you for the opportunity to share the views of the Cyber Security Industry Alliance (CSIA) on improvements to the Federal Information Security Management Act of 2002 (FISMA). CSIA is a group of leading security technology vendors that are dedicated to ensuring the privacy, reliability, and integrity of information systems through public policy, technology, education, and awareness. It is our belief that a comprehensive approach for enhancing the security and resilience of information systems is fundamental to economic security, national security, and sustained confidence in the Internet.

First please allow me to commend this Subcommittee and its parent Committee for the sustained attention that has been given in recent years to the critical objective of strengthening information security within the U.S. federal government. As we have painfully learned, federal systems are frequently vulnerable to cyber attacks, and the oversight by this Subcommittee and full Committee are an important element in holding federal agencies accountable for improved information security as well as highlighting ongoing challenges and vulnerabilities. The 110th Congress now has an important opportunity to amend FISMA to improve the information security climate at our federal government agencies. Even though the last few years have yielded a number of successes, there are certain weaknesses in our government's critical infrastructure which still urgently need to be addressed.

Today's hearing is especially timely given the escalating, large scale information security intrusions and data losses that have occurred at our federal agencies over the past year. As the Committee explores enhancing FISMA, I think that it is particularly important for us to first understand the current evolving threat landscape including the nature and scope of the threats to our government's IT security infrastructure.

According to the Identity Theft Resource Center, the number of publicly reported data breaches rose over 40% in 2007 from the previous year while at the same time exposing over 127 million records in 443 reported data breaches. Additionally, CSIA member company Symantec reveals in its most recent 2007 Internet Security Threat Report (ISTR) that the government sector is the third most targeted sector for global cyber attacks and yet at the same time is wholly responsible for 26 percent of all data breaches that may lead to identity theft.

It has become clear that the infiltration of federal government networks and the possible theft and/or exploitation of information are among the most critical issues confronting our federal government. We've recently become aware of a series of attacks perpetrated by hackers operating through Chinese Internet servers against our computer systems at several federal agencies. Hackers were able to penetrate Federal systems and use "rootkits" – a form of software that allows hackers to mask their presence – to send information back out of federal agency

systems. Last year, the Department of Homeland Security (DHS) reported that it had experienced 844 "cybersecurity incidents" in fiscal years 2005 and 2006. These incidents and statistics clearly underscore that we are all at risk and present clear warning signs that we must devote serious attention to our nation's information security. While progress has been made, much work remains to be done in order to truly secure our government's IT infrastructure.

FISMA has been fairly successful in getting agencies in general to pay closer attention to their information security obligations. Before FISMA, information security was not a top priority at federal agencies. FISMA has been very successful at raising awareness of information security in Congress and federal agencies (for both agency leaders and their IT departments). However, federal agencies scored an average grade of "C-" on 2007's information security report card. As you know, these scores were based on FISMA audits conducted throughout the past year. Last year's average grade was an improvement over 2006 when agencies scored an average of "D+".

Some argue that FISMA does not adequately measure information security: a high FISMA grade doesn't mean the agency is secure, and vice versa. That is because FISMA grades reflect compliance with mandated processes: they do not measure how much these processes have actually increased information security. In particular, the selection of information security controls is subjective and thus not consistent across federal agencies. Agencies determine on their own what level of risk is acceptable for a given system; they can then implement the corresponding controls, and certify and accredit them and thus be compliant and receive a high grade, regardless of the level of risk they have deemed acceptable.

While these grades show slow but steady improvement from past years, challenges obviously remain. There are encouraging signs of progress in the 2007 report, but we continue to be concerned that large agencies like the Defense Department and DHS are still lagging in their compliance. These and other agencies are still lacking in implementing configuration plans, in performing annual tests of security controls, and are inconsistent in reporting incidents. The annual report card does indicate that the federal government overall has made some improvements in developing configuration plans, employee security training, and certifying and accrediting systems.

FISMA does not tell the whole story when it comes to agencies' information security practices. Nowhere is an agency's ability to detect and respond to intrusions measured in FISMA. FISMA is a great baseline log, but clearly much more needs to be done in this area. We need to incentivize strong information protection policies and pursue a goal of security rather than compliance. The FISMA process is a good one, but we need to always ask ourselves if we can make it better as new threats evolve. We believe that optimal security policies would require agencies to monitor networks, test penetration, complete forensic analyses, and mitigate vulnerabilities.

Certainly, we want to avoid a 'check the box' mentality and don't want FISMA to be reduced to a largely paperwork drill among the departments and agencies, consuming an inordinate amount of resources for reporting progress while yielding few genuine security improvements. Unfortunately, in some cases that is what it has become. Some federal agency CISOs are measured on their compliance scores with FISMA, not on whether they have adequately assessed risk in their respective agency or prevented breaches of sensitive information.

Instead, we want agencies to actively protect their systems instead of just reacting to the latest threat with patches and other responses. With the benefit of five years' experience under FISMA and several insightful reports by the U.S. General Accountability Office, it is now possible to identify possible improvements that can address those weaknesses in FISMA implementation that

have now become apparent. With global attacks on data networks increasing at an alarming rate and in a more organized and sophisticated manner, *there is precious little time to lose*

Faced with this urgent need for action, CSIA applauds Chairman Clay for introducing H.R. 4791, the Federal Agency Data Protection Act of 2007. We strongly support this bill. It would undertake the important step of codifying many of the recommended steps that the Office of Management and Budget took in a series of memos to U.S. federal agencies after a series of significant data breaches during the past couple of years. The legislation provides much needed commonsense obligations to require agencies to develop policies and plans to identify and protect personal information, to develop requirements for reporting data breaches, and to report to Congress a summary of information security breaches reported by federal agencies.

We recommend that the proposed legislation also include language requiring that data breaches of information systems maintained by contractors or other sources working on federal projects be promptly notified to the Secretary and the CIO of the contracting agency. Contractor obligations for taking steps, such as notifying affected individuals or providing credit monitoring, may be unclear unless specified in the contract. Federal contractors were responsible for many of the data breaches that agencies reported. CSIA believes that it's important to reaffirm that the Federal Information Security Management Act applies to federal contractors.

We commend the Chairman for also having the insight to incorporate language into this legislation requiring that federal government agencies encrypt, or make unusable and unreadable, personal data and to establish minimum requirements for protection of information on mobile devices.

HR 4791 also prudently establishes security requirements for peer-to-peer networks. CSIA believes that agencies should be required to develop a plan to protect against the risks of peer-to-peer networks, and provide detailed technology and policy procedures they should take. Peer-to-peer file-sharing applications allow computers to exchange information directly without connecting to a central server. Peer-to-peer (P2P) file-sharing allows users to share files online through an informal network of computers running the same software. File-sharing can give users access to a wealth of information but it also has a number of security risks. You could download viruses or other malicious code without meaning to. Or you could mistakenly allow other people to copy files you don't mean to share which greatly increases the possibility of a security breach.

To assist in the Subcommittee's further consideration of H.R. 4791, CSIA offers the additional recommendations below.

1. **Align responsibilities and authorities to vest the Chief Information Officer (CIO) and Chief Information Security Officer (CISO) with specific power over information security. The current authority of Agency CIOs to *ensure* should become the power to *enforce* cost effective measures of security. This must be accomplished by the CIOs of the organization's different units supporting the department-wide CIO.**

- To effectively establish and maintain a comprehensive information security program for federal agencies, CIOs and CISOs need the enforcement authority, budget authority and personnel resources to carry out this essential mission. Funding needs to be allocated to those organizations and facilities that require the most support.

- The senior management of organizations that do not actively support the information security efforts must be held accountable for the failure of the organization to meet its FISMA responsibilities.

2. **Require improvements to assessment, continuous monitoring, and remediation in order to develop a comprehensive approach to information systems security.**

- Agencies need to implement strategies for security monitoring that assesses the health and resiliency of information systems on a regular, *continuous* basis.

- Although NIST issued base-line control updates in December 2006, additional emphasis on evaluation consistency for cyber security readiness among agencies is needed. This is complicated by differences in background and expertise at the Agency Inspector General level.

- Congress should codify CIO/CISO responsibility and authority for testing and continuous monitoring as needed, but more than once a year.

3. **Mandate preparation of a complete inventory of all federal agency IT assets by a certain date.**

- The federal government is responsible for a massive amount of information technology assets that is expanded and maintained by a substantial IT budget. Those assets are located within the U.S. and abroad, within government owned buildings and leased buildings, in the homes of telecommuters and others, and can be stationary and mobile. It is a complicated task to complete a comprehensive inventory, but you can't protect what you don't know about even though an enemy might know about it. Control systems have been added to NIST guidance, but this needs to be incorporated into the law. Although this is presently a requirement, implementation of a complete inventory must be made a priority.

4. **Improve performance measurement and provide incentives to agencies that give information security a high priority.**

- OMB should establish metrics and leading indictors on an annual basis that address agency performance on a 12 to 24 month timeframe. This would provide Agencies with some lead time to identity resources and implement controls to achieve some measure of performance with the identified metrics. Using a security maturity model such as NIST's Program Review for Information Security Management Assistance (PRISMA) would also accomplish the same objectives.

- The large federal agencies and departments are viewed monolithically from the outside. Organizations such as the Departments of Energy, the Interior, or Treasury are viewed as a single organization predicated on the assumption the CIOs have management control over the policies, procedures, and implementation requirements of FISMA. In reality, the operating units must each tailor the requirements and institutionalize good security practices within their organizations. Performance must be measured and collected at both the operating unit and the Agency level.

- With the many competing priorities federal agencies face to deliver mission success in a cost-constrained environment, cyber security is seldom a high priority. Agencies need to be incentivized to provide information security high visibility and a high priority.

Incentives could address a broad range of rewards from public acknowledgement to additional funding or personnel bonuses.

5. **Institutionalize security within federal agency culture.**

- *Training at all levels and functional responsibilities is critical to the success of agencies' information security program.* OMB should establish a CISO Council to meet regularly and report to Congress on the effectiveness of sharing best practices, group purchases of automated tools and training courses, and development a more effective common curriculum for training.

6. **Increase Federal Agency IT Security Funding.**

- President Bush's proposed budget for fiscal 2009 includes $7.3 billion for cyber security efforts -- a 9.8 percent increase from last year. We urge Congress to meet and even exceed these proposed spending levels. According to documents issued by the Office of Management and Budget, five agencies currently rate unsatisfactory in cyber security efforts, based on reports from inspectors general. The Defense Department is still undergoing an audit. Federal agencies submitted planned IT security spending to OMB as part of their budget requests. In order to meet any new and enhanced FISMA requirements, agencies will continue to need sustained and increased IT security funding.

7. **Reaffirm objective assessments of commercially available information technologies.**

- Given that new Internet technologies have the potential to dramatically enhance government performance at a substantially lower cost, FISMA should affirm that government agencies conduct an objective assessment of their security and not fall behind the curve by limiting their procurement options because preconceived compliance concerns prevent efforts to achieve greater efficiencies, better service, and improved security.

8. **Narrow the scope of the privacy definition.**

- We recommend the Committee consider revising the bills current definition of "privacy" to a narrower scope as defined in the California data breach bill in which "Personal information" means the first name or first initial and last name in combination with and linked to any one or more of the following data elements that relate to a resident of California, when the data elements are neither encrypted nor redacted:
    a. Social Security number;
    b. Driver's license number or state identification card number issued in lieu of a driver's license; or
    c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.
    d. The term does not include information that is lawfully obtained from publicly available information, or from Federal, State, or local government records lawfully made available to the general public.

In closing, I commend all of you for highlighting the importance of information security and for examining how we can improve FISMA and federal agency information security practices going forward. FISMA can be strengthened if we develop processes and metrics that truly measure information security and help guide investments in personnel, capabilities, and technical controls that can more effectively secure complex federal computing enterprises. We need to get beyond counting solely on compliance; we need to encourage risk-based approaches to information

security. We need to embrace the public-private partnership that information security requires; and we need to take steps immediately that improve both the policy and the practice of information security. The overriding objective should be to move federal agencies to act in a manner that equates strong information security practices with overall mission accomplishment. We all know what's at stake.

I appreciate the invitation to share my thoughts and recommendations on behalf of CSIA, and I stand ready to engage with our private and government partners on enhancing our nation's information security going forward.

Thank you.

Mr. CLAY. Thank you, Mr. Bennett. I thank the entire panel for their testimony today.

Now we will proceed under the 5-minute rule to questions for the panel. I will recognize the ranking minority member of the full committee, from Virginia, my good friend, Tom Davis. Mr. Davis.

Mr. DAVIS OF VIRGINIA. Thank you, Chairman Clay. I want to thank you for holding this important hearing.

We are here to talk about information security from the Federal perspective. But these are issues and challenges we face at all levels of Government and even as individuals. Secure information is the lifeblood of effective Government policymaking, good program management and a thriving economy. Protecting that information has to be a priority, not an after-thought.

The evolving nature of cyber threats requires constant vigilance. The Federal Government's information security program should be proactive, not reactive. If we keep chasing yesterday's problems, we will never be able to stop tomorrow's sophisticated challenges.

When it comes to information security, all it takes is one weak link to break the data chain. One successful cyber attack could strike a stunning blow to an agency's operations and damage citizens' trust in electronic Government initiatives.

Continued vulnerability puts personal information at risk. The loss of Blackberry service a few days ago reminded us of our dependence on IT, how difficult it is for us to function without it, and how fragile some key systems remain.

One of the best ways to defend against attacks is to have a strong and yet a very flexible protection policy in place, not overly prescriptive. We want agencies to active protect their systems, instead of simply reacting to the latest threat with patches and other responses.

On the Government Reform Committee, I focused on Government-wide information management and security for many years. The Privacy Act and the E-Government Act of 2002 outlined the parameters for the protection of personal information and the Federal Information Security Management Act [FISMA], requires each agency to create a comprehensive risk-based approach to agency-wide information security management through preparedness, evaluation and reporting requirements. It is intended to make security management an integral part of an agency's operation and to ensure that we are actively using best practices to secure our systems.

Certainly, FISMA has its critics. We have heard from some of them today. But I think we also will hear that it still provides the necessary tools to secure our information, and has made information security a priority mention at agencies. We want to avoid that check the box mentality that has been criticized, and we need to incentivize strong information protection policies. We need to pursue a goal of security rather than compliance.

Nearly 5 years after FISMA was enacted, there is always the risk of complacency. The basic FISMA concept and process remains sound. But we should ask if we can make it better. I think we can.

As a start, I introduced legislation requiring timely notice be provided to individuals whose sensitive personal information could be compromised by a breach of data security at a Federal agency. De-

spite the volume of sensitive information held by agencies, there is no current requirement for citizens to be notified if their information is compromised. This legislation passed the House during the 109th Congress. I continue to urge Chairman Waxman to make it a priority this year. I would ask that the two letters I have sent to Chairman Waxman be included in the record, Mr. Chairman.

Mr. CLAY. Without objection, so ordered.

[The information referred to follows:]

Submitted into the record by Tom Davis of Virginia 02/14/08 IP - Hearing

HENRY A. WAXMAN, CALIFORNIA,
CHAIRMAN

TOM LANTOS, CALIFORNIA
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
BRUCE L. BRALEY, IOWA
JOHN A. YARMUTH, KENTUCKY
BRUCE L. BRALEY, IOWA
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
BETTY MCCOLLUM, MINNESOTA
JIM COOPER, TENNESSEE
CHRIS VAN HOLLEN, MARYLAND
PAUL W. HODES, NEW HAMPSHIRE
CHRISTOPHER S. MURPHY, CONNECTICUT
JOHN P. SARBANES, MARYLAND
DENNIS W. KUCINICH, VERMONT

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5051
FACSIMILE (202) 225-4784
MINORITY (202) 225-5074

www.oversight.house.gov

TOM DAVIS, VIRGINIA,
RANKING MINORITY MEMBER

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
JOHN M. MCHUGH, NEW YORK
JON E. SESSIONS, FLORIDA
MARK E. SOUDER, INDIANA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
JOHN J. DUNCAN, JR., TENNESSEE
MICHAEL R. TURNER, OHIO
DARRELL E. ISSA, CALIFORNIA
KENNY MARCHANT, TEXAS
LYNN A. WESTMORELAND, GEORGIA
PATRICK T. MCHENRY, NORTH CAROLINA
VIRGINIA FOXX, NORTH CAROLINA
BRIAN P. BILBRAY, CALIFORNIA
BILL SALI, IDAHO
JIM JORDAN, OHIO

July 27, 2007

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington D.C., 20515

According to a new Government Accountability Office investigation, the Department of Veterans Affairs has lost 53 computers from around the country – computers that could include veterans' sensitive personal information. As you know, I have focused on government-wide information management and security for a long time, and this latest incident simply confirms the need for quick action on proactive security breach notification requirements for Federal agencies.

Unfortunately, this is just the latest case of personal information placed at risk by Federal agencies. Within a little more than a year, a Department of Veterans Affairs employee reported the theft of a laptop that holds more than 26 million records containing personal information; the Census Bureau could not account for more than 1,000 laptops issued to employees and containing sensitive information, and the Department of Agriculture left sensitive data on a Website, putting the personal information of 150,000 individuals as risk.

As you recall, last year we sent a joint request to all cabinet agencies seeking information about data breaches involving the loss of sensitive personal information. The responses listed a wide range of incidents involving data loss or theft, privacy breaches and security incidents. In almost all these cases, Congress and the public would not have learned of each event had you and I had not requested the information. Following the theft of a laptop last year, for example, VA leadership delayed acting for almost two weeks while millions of people were at risk of identity theft. But despite the volume of sensitive information held by agencies, currently no requirement exists that they notify citizens whose personal information may have been compromised.

My bill (H.R. 2124) requires timely notice to individuals whose sensitive personal information could be compromised by a breach of data security at a Federal agency. Under my legislation, the executive branch must establish practices, procedures and standards for agencies to follow if sensitive personal information is lost or stolen and there is a reasonable risk of harm to an individual. The bill provides a clear definition of the type of sensitive information we're trying to protect. It gives agency chief information officers the authority, when appropriate and authorized, to ensure agency personnel comply with information security laws already on the books. Finally, it will ensure costly equipment containing potentially sensitive information is accounted for and secure.

The language in my bill is identical to H.R. 6163, which I sponsored last Congress. Last year, I incorporated identical language into the Veterans Identity and Credit Security Act (H.R. 5835), which you cosponsored and which passed the House last September. That bill, including my language, had strong bipartisan support, with 67 cosponsors from both sides of the aisle.

The Federal government holds sensitive personal information on every citizen, including tax returns, military records, and health records. We need to ensure the public knows when its sensitive personal information has been lost or compromised. I am sure you agree, public confidence in government in this area is essential.

This bill is a critical first step toward limiting the loss of our sensitive personal information. I respectfully request that you join me in moving this important legislation to the full House without delay.

Sincerely,

Tom Davis
Ranking Member

Submitted into the Record by Cong. Tom Davis, Rep. 02/14/08 - I P Hearing

[illegible]

[illegible]

[illegible]

ONE HUNDRED TENTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

Majority (202) 225-5051
Minority (202) 225-5074
Facsimile (202) 225-9974

www.oversight.house.gov

[illegible]

[illegible]

[illegible]

November 19, 2007

The Honorable Henry A. Waxman
Chairman
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C., 20515

Dear Chairman Waxman:

Since I last wrote to you on July 27, Federal agencies have experienced a variety of events involving data loss or theft, privacy breaches, and security incidents. It is likely some of these incidents placed sensitive personal information as risk. As I noted then, however, agencies are not required to notify citizens whose personal information may have been compromised.

My bill (H.R. 2124) would require timely notice to individuals whose sensitive personal information could be compromised by a breach of data security at a Federal agency. Identical language passed the House last September as part of the Veterans Identity and Credit Security Act (H.R. 5835), a bill we both supported.

Given the volume of personal data held by the Federal government, citizens need to know when their sensitive information has been lost or compromised. As I am disappointed the Committee did not take up this legislation, I ask you to take advantage of Congress' return in December to move this important bill to the full House.

Sincerely,

Tom Davis
Ranking Member

Mr. DAVIS OF VIRGINIA. Each year, I have released Federal Agencies Information Security score cards. Despite some improvements, scores for many departments remain unacceptably low. By the way, a lot of the scoring is done by GAO and OMB. It is not just done by our whim.

The Federal Government overall received a C minus, a slight improvement over prior years. I know some don't like to be graded. I have actually had Cabinet secretaries call me to lobby about their grades. And others don't see the value.

But I think most of us agree 5 years later that information security should be a priority at Federal agencies. This is how it should be. The Federal Government has sensitive personal information on every citizen, from health records to tax returns to military records. We need to ensure that the public knows when its sensitive personal information has been lost or compromised. Public confidence in Government in this area is essential.

As we discuss Federal information security, we should focus on the most pressing issues and threats, remain technology-neutral and take care not to disrupt the progress we have made or the progress already underway. Not being technology-neutral, I think, siphons a lot of innovation from this area. That is a major concern with being overly prescriptive, something we have to balance.

In the end, the public demands effective Government and the future of effective Government and security information depends more than ever on a successful future for FISMA.

Thank you, Mr. Chairman.

[The prepared statement of Hon. Tom Davis follows:]

Jim Davis

"Federal IT Security: The Future for FISMA"

Information Policy, Census, and National Archives Subcommittee

Government Management, Organization, and Procurement Subcommittee

2154 Rayburn House Office Building

February 14, 2008 11:30 a.m.

Mr. Chairman, thank you for holding this important hearing. We're here to talk about information security from the federal perspective. But these are issues and challenges we face at all levels of government, and even as individuals. Secure information is the lifeblood of effective government policy making, good program management and a thriving economy. Protecting that information has to be a priority, not an afterthought.

The evolving nature of cyber threats requires constant vigilance. The federal government's information security program should be proactive not reactive. If we keep chasing yesterday's problems, we'll never be able to stop tomorrow's sophisticated challenges.

When it comes to information security, all it takes is one weak link to break the data chain. One successful cyber attack could strike a stunning blow to an agency's operations and damage citizens' trust in electronic government initiatives. Continued vulnerability puts personal information at risk. The loss of Blackberry service a few of days ago reminded us of our dependence on IT, how difficult it is for us to function without it, and how fragile some key systems remain.

One of the best ways to defend against attacks is to have a strong, yet flexible, protection policy in place. We want agencies to actively protect their systems instead of simply reacting to the latest threat with patches and other responses.

On the Government Reform Committee, I have focused on government-wide information management and security for many years. The Privacy Act and the E-Government Act of 2002 outline the parameters for the protection of personal information. And, the Federal Information Security Management Act (FISMA) requires each agency to create a comprehensive risk-based approach to agency-wide information security management, through preparedness, evaluation, and reporting requirements. It's intended to make security management an integral part of an agency's operations,

and to ensure that we are actively using best practices to secure our systems.

Sure, FISMA has its critics. We'll hear from them today. But I think we'll hear that it still provides the necessary tools to secure our information, and has made information security a priority mission at agencies. Certainly, we want to avoid a "check the box" mentality. We need to incentivize strong information protection policies. We need to pursue a goal of security rather than compliance.

And, nearly five years after FISMA was enacted, there's always the risk of complacency. The basic FISMA concept and process remain sound, but we should ask if we can make it better.

As a start, I have introduced legislation requiring timely notice be provided to individuals whose sensitive personal information could be compromised by a breach of data security at a federal agency. Despite the volume of sensitive information held by agencies, there is no current requirement for citizens to be notified if their information is compromised.

This legislation passed the house during the 109th Congress, and I continue to urge Chairman Waxman to make it a priority this year.

[I ask that letters to Chairman Waxman be included in the record]

Each year, I release federal agency information security scorecards. Despite some improvement, scores for many departments remain unacceptably low. The federal government overall received a C minus, a slight improvement over prior years. I know some don't like to be graded, and others don't see the value. But most will agree, five years later, information security is a priority at federal agencies.

And this is how it should be. The federal government has sensitive personal information on every citizen – health records, tax returns, military records. We need to ensure the public knows when its sensitive personal information has been lost or compromised. Public confidence in government is this area is essential.

As we discuss federal information security, we should focus on the most pressing issues and threats, remain technology-neutral, and take care not to disrupt the progress we've made, or the progress already underway.

In the end, the public demands effective government. And the future of effective government and secure information depends more than ever on a successful future for FISMA.

Mr. CLAY. Thank you, and would the ranking member care to ask questions?

Mr. DAVIS OF VIRGINIA. Ms. Evans, let me ask you, the administration has focused unprecedented attention on the mundane but the very essential tasks of improving Federal management practices, including a focus on expanding electronic Government. The President's management agenda rates agencies' efforts on E-Gov initiatives, OMB requires quarterly reports, yet we still have a long way to go before things are secure.

Do you have any advice or recommendations for the next administration of things they should prioritize?

Ms. EVANS. I have a lot of advice. But in particular, I think that the areas that we focused on and the specific processes are good foundational activities that I think any administration would want to continue. For example, on the score card, one of the things that we look at, and on a quarterly basis as required by the guidance that has been outlined in FISMA, is the plan of actions and milestones which really is the constant assessment of risk.

If an agency is in the check the box mentality, then we are going to get the results that the other panelists, my colleagues, have talked about. But if the agency head and the CIO are really evaluating the new technologies, the services that they have, that process, that monthly looking at things, the daily looking at things and then making sure that you have an adequate way to then address it I think is a good practice to carry forward. We call it certification and accreditation overall, we call the quarterly reports, plan of actions and milestones, but what it really is is getting to the culture of managing the risk.

Mr. DAVIS OF VIRGINIA. Have you found any agencies that just check the box and literally don't have the substance behind checking it?

Ms. EVANS. I think that there are mixed results, as we have said in our reports in the past. I work very closely with all the agencies, especially through the CIO council. I do and am concerned that we balance the compliance aspect of this legislation and any legislation that we have against achieving the actual results. So I would say there are mixed results and it depends on the leadership and the CIO in particular of how they are managing that information security program within the department.

Mr. DAVIS OF VIRGINIA. The report cards are not perfect, but right now, nobody else is keeping track, at least up here, over what is happening. If you don't give a report card or at least give some public embarrassment, there is no appropriations penalty to be paid or anything else. Ultimately it has to be directed from OMB. The executive branch doesn't need us involved in a perfect world. We have to make this a priority.

But managers down below, given limited funds, generally want to accomplish their mission first. Many of them would just as soon take the risk of a data breach to be able to accomplish things, and if something happens, hopefully it won't happen on their watch. That is one of our concerns.

Ms. EVANS. And I would agree with you and I think that is what we have done through the criteria that we manage and look at on a quarterly basis through the E-Government Score Card on the

President's management agenda. It is looking at all and everything that takes into consideration for a good information technology program in a department. If you master those management skills, then you have the foundation to go forward to support any program.

All of this is about getting good program results and making sure that you have public confidence in your services. So you have to do many things in order to do that in this environment. The way to provide those services is through the use of information technology.

Mr. DAVIS OF VIRGINIA. Mr. Paller, part of your testimony approaches Federal IT from an international perspective. How do we rank when you compare us with government IT security in other countries?

Mr. PALLER. First, the breach bill that you talked about, this is going to do a lot of good. Because people respond when they have to make something public in ways they don't even think about.

Mr. DAVIS OF VIRGINIA. No question. The tendency is to sweep it under a rug, fully investigate, make sure you get your spin on it. That is just natural. We do the same, by the way, we are no different than the executive agencies.

Mr. PALLER. In almost all areas, we are stronger than other governments. The one place we fall way behind is in information sharing. The British figured out how to do that. They actually copied something we had called the NSIE, and spread it and we didn't copy what we had and we built this thing called ISACS that just don't work. So they are way ahead on information sharing.

But in terms of actually securing Government systems, we are not way behind anyone.

Mr. DAVIS OF VIRGINIA. We are also more of a target than most government systems, aren't we?

Mr. PALLER. We are getting hurt more, the British equally, the Australians, too. These nation-state attacks are enormous. the head of MI–5 actually just did a letter that it is all spreading to businesses now. If you do business in China, you are being just destroyed with cyber attacks.

Mr. DAVIS OF VIRGINIA. I hope we can sit down and work some language out that and can all agree on this. Because a cyber Pearl Harbor or something of that nature would just be awful. And at that point, you would say, where have we all been on this. And a lot of us have been working on this for a long time. It is not easy.

Can I just ask one other question? Mr. Wilshusen, some have suggested that standardizing IG audits, their practices in the area of information security, would help reduce the discrepancy between the agency grades, their compliance with the act and their information security practices. Is it feasible to standardize audit practices? Do you agree with that proposal?

Mr. WILSHUSEN. I think audits and in particular, with the independent IG evaluations, we have noted in the pst that they have been inconsistent, the scope and methodology of their evaluations vary across agencies. And the form and content of the reports differs significantly from just repeating or presenting the information on the FISMA template that OMB has established to coming up with real conclusions and findings and issues on these security deficiencies at those agencies.

So by having these evaluations of performance in accordance with Government auditing standards, for example, that could elevate and raise consistency in the content of those evaluations.

Mr. DAVIS OF VIRGINIA. Thank you.

Mr. CLAY. Thank you, Mr. Davis.

Mr. Paller, I am very interested in your testimony's support of prioritizing the testing and evaluation activities that are carried out by agencies on a regular basis. Thus, I have a few practical questions on how would you get there. Does current guidance from NIST, such as S.P. 853, provide a blue print for adequate security and should this guidance simply be made mandatory and binding on agencies?

Mr. PALLER. No, and hell, no. It is a catalog of everything anybody ever thought of that might help security, 853. Not even the audit guide, this is it. There is a parallel in the commercial world that is what you actually have to do to secure all the credit cards. Because the credit card industry says, we are going to stop losing it. This looks smaller. And this one, in all of this, firewalls are a really important part of security, lock the door, firewalls the door. In all of this, one-200th of it talks about firewalls. In the real one, one eighth. So 12½ percent talks about it.

If you know security, you actually know security, not know about writing about security, but actually doing it, no, 853 is silly.

Mr. CLAY. How can new guidance or security controls be added in a real-time environment?

Mr. PALLER. I think again, the payment card industry does it. These are updated regularly. There is a massive new attack on Web applications. They used to go against Windows and the other things. Now they are going against every Web site.

Well, this has nothing, it tells you nothing about doing that. But this one is updated very regularly, almost quarterly. It is not hard. All you do is you set up a council of the people who actually have to protect systems, say, what are you doing and then get them to agree, 10 or 12 of them, they agree and you write it up. It really isn't impossible. It is not easy, but it isn't impossible.

Mr. CLAY. You also referred to the Air Force contracting which had required vendors to deliver minimum security configurations for a system. Should a contractual mandate along these lines, with requirements defined by OMB and the Federal Acquisition Council be required under FISMA?

Mr. PALLER. That is actually Karen's, she has done a lot of wonderful things. Taking what the Air Force did and making it a Federal mandate is the biggest, single biggest thing in improving security we have ever done as a country.

Mr. CLAY. Is that what Ms. Evans is pushing?

Mr. PALLER. Yes, what Ms. Evans has done.

Mr. CLAY. Would we have the problem of technology moving ahead too quickly for regulations to keep up?

Mr. PALLER. No. The Air Force, for example, has this absolute mandate. You have to do it this way. And if you compare the Air Force's new computers with every other agency, they are ahead of the other agencies. So you can't say they are behind technologically when they actually have the most advanced technology and yet

they are meeting the standard. It is because they do it together that they get all the advanced technologies.

Mr. CLAY. Thank you for that response.

Let me ask Mr. McConnell, can you tell us how laws like FISMA and Clinger-Cohen have altered the information security landscape over the past decade, and if there areas in which we should try to harmonize the provisions in order to improve security?

Mr. MCCONNELL. Yes, sir. I think there have been three beneficial effects of FISMA and Clinger-Cohen. They have increased the level of attention that is paid to information security, they create a management structure that can be used to manage it, and they have encouraged integrating security into the overall program management. So you have a well-managed program that includes good security.

I think what is needed at this point is for the executive branch to take full advantage of the authorities and structure that you have provided. I have seen that work in the past across administrations. The Clinger-Cohen bill set out authorities in a management structure that was passed during the Clinton administration. And now the current administration has really exercised those authorities in a significant way.

I think as far as harmonization, the law that is probably the most in need of harmonization and updating that is under this committee's jurisdiction is the Privacy Act. That is the Privacy Act of 1974. And that as you can imagine, there is much that could be done to harmonize that with other things that have happened.

Mr. CLAY. Can you explain in further detail why an independent audit would hinder agency efforts to root out security vulnerabilities? Isn't one of the problems with FISMA related to the current evaluations having little consistency or applicability across agencies, making it a paperwork exercise?

Mr. MCCONNELL. I would agree that the current evaluations are inconsistent and that they often focus on paperwork. But I don't think those two aspects are necessarily connected. You have inconsistency because you have inconsistent evaluation criteria and processes. Whereas the paperwork is looking at a compliance, box checking, rather than on operational security, as Mr. Paller was saying, let's just get the stuff done.

So you could have consistent processes, but still have the paperwork focus. The concern that I have about the mandatory audit is that you just exacerbate the compliance mentality. Everybody at that point is in a CYA thing, trying to make the audit right. So I think you need to have consistent evaluation criteria, independent evaluation criteria, but I don't recommend making it an audit.

Mr. WILSHUSEN. Mr. Chairman, may I please comment?

Mr. CLAY. Sure.

Mr. WILSHUSEN. One thing, and i Just want to make sure that we are clear on if we are talking about the annual independent IG evaluation or audit, if that is the change in H.R. 4791, versus the testing that may be done by the agencies. One thing that is important, if we go to an audit by the IG as part of the annual evaluation, is to make sure that the audit focuses on and the auditors conclude on the effectiveness of the information security controls,

rather than making it merely compliance with the provisions of the act.

And so it is important to direct the focus of the audit toward evaluating effectiveness as the IGs and auditors do as part of the consolidated financial statement or the audits of the agencies' financial statements. And that is why you have a disparity between why certain agencies are reporting increased performance versus the various metrics established by OMB for FISMA reporting versus those audit results of the effectiveness of controls.

So there is a distinction there to try to make the annual IG evaluation by making it in accordance with audit standards and assuring that the auditors conclude on the effectiveness of controls, not merely compliance with the act.

Mr. CLAY. And these should be independent audits?

Mr. WILSHUSEN. Absolutely.

Mr. CLAY. Yes.

Mr. WILSHUSEN. And that is separate from the agencies that are also required under FISMA to test and evaluate the effectiveness of their controls. And that would be all their controls, management, operational, technical controls, on a frequency based on risk. We have found problems with that process being implemented by the agencies. But those are two separate issues, once performed independently by the IG or other auditors, others. The security tests and evaluations required as part of an agency information security program is performed by agency personnel or their contractors.

Mr. CLAY. Thank you for that response.

Mr. Bennett, a critical element of FISMA is for agencies to develop a risk assessment of their systems in order to develop or integrate effective security policies and applications for them. With this in mind, please characterize the vendors' roles and responsibilities in developing and implementing secure networks and applications throughout an agency.

Mr. BENNETT. Yes, Mr. Chairman. The vendor should be responsible for understanding the agency's enterprise architecture and the operating environment to assure that their solutions will not disconnect or break the systems that are currently in place. While Government and their contractor personnel, support personnel are ultimately responsible for the support and operation of the infrastructure, only the vendors of these enterprise solutions really understand the protocols and underlying infrastructure requirements that will allow these products to work securely and as designed.

This means that implementation, testing and integration of cyber security and risk in the mission achievement is the responsibility of the vendor in the larger context of the agency framework and budget.

Mr. CLAY. Is the mitigation of risk a shared duty or responsibility between both agency personnel and the vendor community?

Mr. BENNETT. Yes, absolutely it is a shared responsibility, to the extent that the vendors' products should work as advertised. The agency is solely responsible for the determination of how much risk they are willing to take and NIST guidelines do provide some guidance in this area.

But once mitigation plan has been decide, the agency should have every expectation that the solutions that have been purchased performed as advertised.

Mr. CLAY. In actuality, and anybody on the panel can answer this, how does it actually work between vendor community and agency? Is it pretty seamless? Is it a turf war? What have you found? Ms. Evans, you can start.

Ms. EVANS. I would like to take the opportunity to first talk about that. I applaud the answer of my colleague at the other end of the table. But when it ultimately comes down to it, the agency head is ultimately responsible for the services that they procure and the contracts that they let. So it is the responsibility of the CIO, which is outlined in the statute, to ensure that we manage that risk appropriately.

So you have to have very clear and open communications. You have to make sure that the contact is very clear as to what the roles and responsibilities are. But when it is said and done, the American people hold us, the executive branch, accountable for our actions and for our services. So I believe that what the administration has done with our policies and the actions that we are taking is trying to make that very clear and using the tools that we have in place to leverage our buying power, so that it is clear to us and clear to those who choose to provide the services for us what those expectations are, what the risks are and how those products need to work in our environment.

Mr. CLAY. Thank you.

Mr. Wilshusen.

Mr. WILSHUSEN. I would just like to add, FISMA requires that the agency is responsible for the security over the systems that are operated on its behalf by third parties and contractors. It should be an integral part of the agency's information security program.

However, we have found in our report that we issued back in, I think it was April 2005, that many of the agencies did not have adequate policies or actually monitoring the effectiveness of security over systems operated by contractors. So Ms. Evans is absolutely correct, it is important that contracts be, or that the requirements for information security be specified in the contracts, so that the contractors know what to do. But there is also that other side of the agency taking responsibility to assure that the contractors are upholding their end of the bargain and implementing the security in accordance with the contract requirements and Federal requirements.

Mr. CLAY. Thank you.

Mr. Paller.

Mr. PALLER. We train 14,000 people a year. Lots of them are Federal people, lots of them are contractors, lots of them are Boeing people. They can't figure this out on the fly. What Ms. Evans is talking about, contracting for what you want, the fact that we don't do that today is one of the two biggest flaws in all of our Federal security. What we do is we throw it over the wall to these contractors. And then when we find out there was something extra we needed to do for security, they say, well, that is another $100 million. Then we have to make choices between spending the extra money or not.

We have to change the way we buy products, to buy it with security baked in, rather than getting caught. That happens with our third party, our software. Right now, if somebody does a software development for us and we find a major security flaw in it, we have to pay them to now go and we have to negotiate with them and now they are busy and they have something else to do. The whole contracting mechanism is, give it away and then, oh, shoot, security, we should have asked you for that. So what Ms. Evans is talking about is not a lightweight thing. It actually matters.

Mr. CLAY. Do you think in the President's proposed $70 billion budget for IT, do you think there are some built-in protections for that, for that security element?

Mr. PALLER. No, the contracting officers don't like this topic. So when the guys want to put it into contacts, am I being bad?

Ms. EVANS. No, you go ahead. [Laughter.]

Mr. CLAY. You are doing fine. Please proceed.

Mr. PALLER. The contracting officers don't like it and so when the technical person who knows what he wants goes to the contracting officer and says, can we put that in, he says, well, you are not being specific enough. And then it is gone.

Ms. EVANS. But I have good news. I bring good news, which is, we have, as I stated in my testimony, we have been working with the Federal Acquisition Council to make modifications to the FAR to do things like what we have done with the Federal Desktop Core Configuration. So the FAR will be amended to then include the common security configurations, which makes it a mandatory clause. That clause, that language is to be published in the Federal Register no later than Tuesday.

So we understand where the performance gaps are. We know we have to follow through in our contracts to ensure that we can hold ourselves as well as the contractors accountable. So if you follow this example through, we gave agencies guidance last year, last June. All new contracts were to have this language in it if you were providing these types of operating systems or you were going to provide products that were going to operate on these operating systems.

What we are following through now is making sure that we will be successful in spite of ourselves, because this will be in the FAR. It will go forward that way. So a lot of these things are now coming into place where the vendors now are like, OK, so what does this mean that I have to provide certification? That is the point of what NIST has done by having this program out which is dealing with—the acronym is S-CAP, but in essence what it does is validate that those security settings stay set when you bring them into your environment.

So a vendor, when you bring in new tooling to your environment or a new application or anything, you run this tool. And it is going to tell you, against those 700 settings, what changes and what didn't. It gives you a percentage. We are talking 100 percent right now. We told the agencies that they had to comply with this. There is no, like, give me 80 percent or so. It is zero or 100.

Then we thought, OK, from that perspective, how would that really go forward. We have agencies that can tell you exactly how many desktop have these operating environments and out of the

700, 5 are problematic and they know exactly now what applications that affects.

We couldn't do that before. So now when you know what that is, you can now put in compensating controls. These lay the good foundations for an information management program. But the key was to ensure that the procurement cycle, and as these products and applications come into our environments, that they too are aware and that they are certifying against that environment.

Mr. CLAY. Will you provide us with the language?

Ms. EVANS. Absolutely.

Mr. CLAY. Thank you so much.

Mr. McConnell, did yo have anything to add?

Mr. MCCONNELL. I think this has been pretty well discussed, sir.

Mr. CLAY. Mr. Bennett, one final question. You mentioned incentives for agency security performance in your testimony. I would like to explore that idea of a carrot and stick approach. Would incentives such as permitting agencies that receive an unqualified or clean independent audit to be audited only every other year be appropriate, and conversely, would penalties for an agency such as losing procurement funding until deficiencies are remedied be an effective tool?

Mr. BENNETT. Yes, Mr. Chairman. I think that might work and should be given serious consideration and should be counter-balanced by the concept that if there is inadequate performance, that the frequency of audits should be increased so that it works both ways and truly becomes a carrot with also a stick.

Mr. CLAY. Thank you so much.

Do any other panelists have anything to add?

Mr. PALLER. I just wanted to connect the dots to Boeing. Everything we are talking about, about compliance, spending all this money, not doing security, I am getting calls all the time, they are just discovering it, does this really mean us, too? So everything we are talking about, about cleaning it up, is about to come back across the entire Defense industrial base, because a few months ago, they found out that the Chinese had gotten deeply into most of their computers as well. So they are now part of the game, and they are subject to all of this and people saying, well, let's make the FISMA-compliant, and all this discussion about paperwork and money wasted, it is all about what we are going to do to the contractors.

Mr. CLAY. So they are watching with a keen eye?

Mr. PALLER. They are going to scream when it hurts.

Mr. CLAY. They are going to scream when it hurts.

Thank you so much, Mr. Paller. Ms. Evans.

Ms. EVANS. On the evaluations or audits, or whatever we end up calling it, I do think that it is important, again, that it is a balance of what we are looking at and the carrot and stick approach. This is something that in my own position that I am sure you guys manage with, as I do, is that we need to be careful about the compliance versus the actual results that we are trying to achieve. Putting timeframes on these things also could drive certain behavior that we may not necessarily want either.

I really believe it gets down to, it is a culture of constantly evaluating the risks associated with the information that you have. And

you know, to take away procurement authority or to take away money in some cases you might have to add money in order to fix these types of activities, because it is so pervasive.

I really believe the way the administration puts together the budget, how we evaluate the capital planing, how we send this stuff forward, really allows the agencies to focus on managing that on a daily basis. It is not a time, it is not a quarter, it is not a year, it is not biannually. Agencies have to do this on a daily basis. It has to be a culture of managing risk on a daily basis.

Mr. CLAY. Thank you so much for that response, Ms. Evans.

Let me thank the entire panel for today's hearing and your testimony. We certainly appreciate your participation in this hearing.

That concludes this hearing. Hearing adjourned.

[Whereupon, at 12:40 p.m., the subcommittees were adjourned.]

○