COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE?

HEARING

BEFORE THE

SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

NOVEMBER 19, 2002

Serial No. 107–240

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE
89–165 PDF WASHINGTON : 2003

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. McHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LaTOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, Jr., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
——— ———

———

BERNARD SANDERS, Vermont (Independent)

Kevin Binger, *Staff Director*
Daniel R. Moll, *Deputy Staff Director*
James C. Wilson, *Chief Counsel*
Robert A. Briggs, *Chief Clerk*
Phil Schiliro, *Minority Staff Director*

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

STEPHEN HORN, California, *Chairman*

RON LEWIS, Kentucky
DOUG OSE, California
ADAM H. PUTNAM, Florida
JOHN SULLIVAN, Oklahoma

JANICE D. SCHAKOWSKY, Illinois
MAJOR R. OWENS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York

Ex Officio

DAN BURTON, Indiana

HENRY A. WAXMAN, California

Bonnie Heald, *Staff Director and Chief Counsel*
Dan Costello, *Professional Staff Member*
Chris Barkley, *Clerk*
Michell Ash, *Minority Counsel*

CONTENTS

COMPUTER SECURITY IN THE FEDERAL GOVERNMENT: HOW DO THE AGENCIES RATE?

TUESDAY, NOVEMBER 19, 2002

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY, FINANCIAL
MANAGEMENT AND INTERGOVERNMENTAL RELATIONS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10 a.m., in room 2154, Rayburn House Office Building, Hon. Stephen Horn (chairman of the subcommittee) presiding.

Present: Representatives Horn and Lewis.

Staff present: Bonnie Heald, staff director; Henry Wray, senior counsel; Dan Daly, counsel; Dan Costello, professional staff member; Chris Barkley, clerk; Ursula Wojciechowski, staff assistant; Michelle Ash, minority counsel; and Jean Gosa, minority clerk.

Mr. HORN. This hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

Federal agencies rely on computer systems to support critical operations that are essential to the health and well-being of millions of Americans. National defense, emergency services, tax collection and benefit payments will all rely on automated systems and electronically stored information. This technology has greatly streamlined government operations. Yet without proper security measures, Federal computers are highly vulnerable to cyber attacks. These attacks are dramatically increasing in volume and sophistication. Last year the number of cyber attacks rose 71 percent above the previous year. In addition, they are more complex, affecting government and nongovernment computers alike.

Earlier this year, a British computer administrator penetrated 100 U.S. military computers, shutting down networks and corrupting data at the National Aeronautics and Space Administration and at the Pentagon. Equally disturbing, the hacker successfully attacked these sensitive systems by using software that was readily available on the Internet. Threats such as this demand that the Federal Government move quickly to protect its critical computer systems.

This is the subcommittee's third annual report card and we are now sending it out and we'll go into questions on it later. This subcommittee will be—this was the third annual report card, and we have been grading executive branch agencies on their computer security efforts. I am disheartened to announce that again this year the government has earned an overall grade of F for its computer security efforts. Despite the administration's welcomed focus on this important problem, 14 agencies scored so poorly that they earned individual grades of an F. The Department of Transportation lags at the bottom of the scorecard, earning an appalling 28 points out of a possible 100 on the subcommittee's grading systems.

At the top end of the report card, I am pleased to note that the Social Security Administration continues to be a shining example of sound leadership and focused attention toward solving this important problem. Earning a score of 82, the Social Security Administration's grade goes from a C-plus to a B-minus. This agency was the first to become Y2K compliant in 1999, and I have no doubt that it will also be the leader in the government's effort to protect its critical computer systems. Hopefully, the Department of Transportation and all other failing agencies will benefit from the experience and expertise of today's witnesses.

September 11, 2001 taught us that we must be prepared for attack. We cannot allow government operations to be compromised or crippled because we failed to heed that lesson.

[The prepared statement of Hon. Stephen Horn follows:]

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
MINORITY (202) 225–5051
TTY (202) 225–6852

Opening Statement
Chairman Stephen Horn, Chairman
November 19, 2002

This hearing of the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations will come to order.

Federal agencies rely on computer systems to support critical operations that are essential to the health and well being of millions of Americans. National defense, emergency services, tax collection and benefit payments all rely on automated systems and electronically stored information. This technology has greatly streamlined government operations. Yet without proper security measures, federal computers are highly vulnerable to cyber attacks. The volume and sophistication of these attacks are dramatically increasing. Last year, the number of cyber attacks rose 71 percent above the previous year. In addition, they are more complex, affecting government and non-government computers alike.

Earlier this year, a British computer administrator penetrated 100 U.S. military computers, shutting down networks and corrupting data at the National Aeronautics and Space Administration and at the Pentagon. Equally disturbing, the hacker successfully attacked these highly sensitive systems using software that was readily available on the Internet. Threats, such as this, demand that the federal government move quickly to protect its critical computers from disruption.

This is the subcommittee's third annual report card, grading executive branch agencies on their computer security efforts. I am disheartened to announce that again this year, the government has earned an overall grade of "F" for its computer security efforts. Despite the Administration's welcomed focus on this important problem, 14 agencies scored so poorly that they earned individual grades of an "F." The Department of Transportation rests at the bottom of the scorecard, earning an appalling 28 points out of a possible 100.

On the top end of the report card, I am pleased to note that the Social Security Administration continues to be a shining example of sound leadership and focused attention toward solving this important problem. Earning a score of 82, the Social Security Administration's grade rose from a "C-plus" to a "B-minus." This agency was the first to become Y2K compliant in 1999, and I have no doubt that it will remain the leader in the government's effort to protect its critical computer systems. Hopefully, the Department of Transportation and all other failing agencies will benefit from the experience and expertise of today's witnesses.

September 11, 2001, taught us that we must be prepared for attack. We cannot allow government operations to be compromised or crippled because we failed to heed that lesson.

I welcome our witnesses today and look forward to your testimony.

Mr. HORN. I'd ask the vice chairman, Mr. Lewis of Kentucky, if you'd like to have an opening statement, why——

Mr. LEWIS. Thank you, Mr. Chairman. Well, I just want to say one thing. At the end of this term, the American taxpayer will be losing a man that has been in the front lines of looking out after their interest and putting pressure on the government to be efficient and to use taxpayer dollars wisely. And, Mr. Chairman, it certainly will, again, be a sad day for the American taxpayer and it'll be a sad day for all of us to see you retire, but thank you for your great service.

Mr. HORN. Thank you very much, Ron. That's nice of you. You've been a good partner.

I'm now going to bring in the witnesses and their assistants and we'll have them take the oath. This is an investigative committee and that's the way we operate. If you'll stand and raise your right hands. And your assistants behind you, the clerk will note all of the names there and put in the hearing record.

[Witnesses sworn.]

Mr. HORN. The clerk will note and take the names. Thank you.

And we will now start with the presentation, and the presentation is simply down the agenda line, and we start with Mark A. Forman, Associate Director, Information Technology and E-Government, Office of the President's Management and Budget.

Mr. Forman, we're glad to see you again.

STATEMENTS OF MARK A. FORMAN, ASSOCIATE DIRECTOR, INFORMATION TECHNOLOGY AND E-GOVERNMENT, OFFICE OF MANAGEMENT AND BUDGET; JAMES B. LOCKHART III, DEPUTY COMMISSIONER AND CHIEF OPERATING OFFICER OF SOCIAL SECURITY, SOCIAL SECURITY ADMINISTRATION; KENNETH M. MEAD, INSPECTOR GENERAL, DEPARTMENT OF TRANSPORTATION; RICHARD D. PETHIA, DIRECTOR, CERT COORDINATION CENTER; AND ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY, U.S. GENERAL ACCOUNTING OFFICE

Mr. FORMAN. Good morning, Mr. Chairman and Mr. Lewis. Before I begin, I would also like to acknowledge the significant role that you've played in the last decade on IT issues. Through your leadership we've all witnessed a substantial increase in attention and efforts to improve the Federal Government's management of information technology. You've captured the attention of senior policy officials across agencies, challenged administrations, and, as a result, have helped focus on an understanding of the serious issues, particularly IT security, financial management and the year 2000 conversion. Thank you for your work in these areas.

I also want to acknowledge the work of my lead security analyst, Glenn Schlarman, who will be leaving OMB to work at a department at the end of the year. Glenn has led OMB's work in cyber security and related information policy since the mid-1990's and deserves much credit for the progress made in this area by Federal agencies.

Mr. Chairman, we all know that our Federal Government's IT security problems are serious and pervasive. However, I'm pleased to report today that while problems persist, several agencies are demonstrating progress due in large part to your leadership.

Since the last hearing in March, a number of achievements have been made toward improving the Federal Government's IT security: First, the combination of the Security Act reporting requirements, OMB's reporting instructions, and agency plans of actions and milestones have resulted in a substantial improvement in the accuracy and depth of information provided to Congress relating to IT security. In addition to IG evaluations, agencies are now providing the Congress with data from agency POAMs, the plans of action and agency performance against uniform measures.

Second, OMB developed and issued objective IT security management performance measures which were the basis for the most recent agency reports and plans of action.

Third, we developed a governmentwide assessment tool based primarily on the National Institute of Standards and Technology's technical guidance and the GAO's Federal Information Systems Control Audit Manual.

Fourth, to ensure successful remediation of security weaknesses throughout an agency, every agency must now maintain a central process through the CIO's office to monitor agency compliance.

Fifth, we have developed additional guidance on reporting IT security costs.

Sixth, several agencies have demonstrated mature IT security management practices.

Seventh, governmentwide on-line IT security training and course work is being made available and used.

And, eight, deployment of cross-agency E-authentication capabilities is occurring.

As we move into the second year of actual reforms built around the Government Information Security Reform Act and based primarily on agency and IG reports submitted in September, integration of security into agency budget processes and recently updated and submitted IG security plans of action and milestones, OMB has conducted an initial assessment of the Federal Government's IT security status. Due to the baseline of agency IT security performance identified last year, we are now in a position to more accurately determine where progress has been made and where problems remain.

Having objective performance measurements has improved the quality process, and I'd like to say there are five good news items we've found in our review:

First, more departments are exercising greater oversight of their bureaus.

Second, at many agencies, program officials, CIOs, and IGs are engaged in working together.

Third, the inspectors general have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to us in the process.

Four, more agencies are using their plans of action and milestones as authoritative management tools to ensure program assistant level IT security weaknesses, once identified, are tracked and corrected.

And, fifth, OMB's conditional approval or disapproval of agency IT security programs has resulted in senior executives at most agencies paying greater attention to IT security.

The bad news is that as we predicted in our previous testimony, the more IT systems that agencies and IGs review, the more security weaknesses we're finding. Our initial analysis reveals that while progress has been made, there remain several significant weaknesses:

First, many agencies find themselves faced with the same security weaknesses year after year. They lack system level security plans and certification. Through the budget process OMB is assisting agencies in prioritizing and reallocating funds to address these problems.

Second, some IGs and CIOs have vastly different views of the state of the agency security programs. Although some agencies have already acted to address more rigorous findings, OMB will highlight such discrepancies in our feedback the agency has.

Third, many agencies are not adequately prioritizing their IT investments, and therefore are seeking funding to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

I'd like to talk a little bit about six common weaknesses we identified in the IT security report to Congress last year:

First, lack of agency senior management attention to security. In addition to conditionally approving or disapproving agency IT security programs through private communication between OMB and each agency head, we have used the President's Management Agenda Scorecard to continue to focus attention on serious IT security weaknesses. Through the scorecard, OMB and senior agency officials are monitoring agency progress on a quarterly basis.

Second, nonexistent IT security performance measures, as I referenced earlier, also address the performance of officials charged with implementing specific requirements of the Security Act. These measures are mandatory and represent the minimum matrix against which agencies must track and measure performance and progress.

Third, poor security education awareness. As in my testimony, the administration's electronic government initiative called E-Training will incorporate additional security courses, and of course agencies are using traditional classroom-style training.

While OMB can and will continue to assist agencies with their efforts in addressing the security weaknesses, but the responsibility and the ability to fix these weaknesses ultimately lies with the agencies.

I'd like also to address some additional areas for attention. OMB, the President's Critical Infrastructure Protection Board, Federal agencies, and others are addressing a number of other significant IT security issues. The administration strives to assure that disruptions of the Federal IT systems are infrequent, of minimal duration, manageable, and cause the least damage possible. In this regard, we're essentially addressing two types of threats: organized and ad hoc.

We'll assure that Federal agencies undertake effective systems management practices with tools and training to ensure timely deployment and continued maintenance of security of IT systems. But countering sophisticated organized threats is far more complex. The development of a governmentwide enterprise architecture is a central part of the administration's IT management and the electronic government efforts. Accordingly, the administration will use this to better prioritize and fund Federal Government security needs.

I run through a number of other additional comments in my testimony. But let me conclude by saying, Mr. Chairman, again, I'd like to express the administration's appreciation for your untiring leadership on IT security and government IT management in general.

Mr. HORN. Thank you.

[The prepared statement of Mr. Forman follows:]

STATEMENT OF
MARK A. FORMAN
ASSOCIATE DIRECTOR FOR INFORMATION
TECHNOLOGY AND ELECTRONIC GOVERNMENT
OFFICE OF MANAGEMENT AND BUDGET
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES
November 19, 2002

Good morning, Mr. Chairman and Members of the Committee. Thank you for inviting me to discuss the status of the Federal government's IT security. As you know, year two of the Government Information Security Reform Act (Security Act) came to a close with the submission of agency and Inspector General reports in September. For the purposes of today's hearing, I will provide the Committee with OMB's initial analysis of the Federal government's IT security progress in fiscal year 2002.

Before I begin, I would like to first acknowledge the significant role you have played in the last decade on IT issues. Through your leadership we have all witnessed a substantial increase in attention and efforts to improve the Federal government's management of IT. You have captured the attention of senior policy officials across agencies, challenged Administrations, and as a result have helped to raise focus and understanding of these serious issues, particularly IT security and Y2K.

We all know that our Federal government's IT security problems are serious and pervasive. However, I am pleased to report today that while problems persist, several agencies are demonstrating progress, due in large part to your leadership.

Government-wide Steps Taken to Improve IT Security

Since the last hearing in March, a number of achievements have been made toward improving the Federal government's IT security.

1. Provided Congress with Information Requested for Proper Oversight. The combination of the Security Act reporting

requirements, OMB's reporting instructions, and agency plans of action and milestones (POA&Ms) have resulted in a substantial improvement of the accuracy and depth of information provided to Congress relating to IT security. In addition to IG evaluations, agencies are now providing the Congress with data from agency POA&Ms and agency performance against uniform measures.

2. Developed IT Security Management Performance Measures. OMB issued updated reporting instructions (M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones") to Federal agencies which included objective performance measures. Both agencies and IGs were directed to report the results of their reviews and independent evaluations against those measures. These measures tie directly to the IT security requirements in the Security Act.

3. Developed Government-wide Assessment Tool. The National Institute of Standards and Technology (NIST) developed a security questionnaire in 2001 which greatly assisted agencies in performing self-assessments of their IT systems. This questionnaire was based primarily on NIST technical guidance and the General Accounting Office's Federal Information System Controls Audit Manual and allows agencies to assess the management, operational, and technical controls of their systems. Agencies were directed through OMB guidance to use this document as the basis for conducting their annual reviews under the Security Act. Under NIST's leadership, this questionnaire was automated this year. Agencies now have a free automated tool to assist them in conducting their annual reviews. The tool facilitates IT security reviews while improving the quality of the overall process.

4. Enforcement of Plans of Action and Milestones. This spring, OMB met with agencies (CIO and IG office) to discuss the status of and address deficiencies in their POA&M efforts. Agencies are required to develop POA&Ms for every program and system where an IT security weakness has been found. These plans must be developed, implemented, and managed by the agency official who owns the program or system (program official or Chief Information Officer (CIO) depending on the system) where the weakness was found. To ensure successful remediation of security weaknesses throughout an agency, every agency must maintain a central

process through the CIO's office to monitor agency compliance. OMB has and will continue to reinforce this policy through the budget process and the President's Management Agenda Scorecard.

5. Developed Guidance on Reporting IT Security Costs. OMB, through Circular A-11 on budget preparation and submission, provided agencies additional guidance in determining IT security costs of their IT investments.

6. Mature IT Security Management Practices. A handful of agencies have demonstrated the maturity of their agency-wide plans of action and milestone (POA&M) process to track and manage remediation of their IT security weaknesses.

7. Government-wide IT Security Training Opportunities. Through the Administration's electronic government initiative, e-training, IT security courses will be available to all Federal agencies by December. These initial courses are targeted to CIOs and program managers, with additional courses to be added for IT security managers, and the general workforce.

8. Deployment of E-authentication Capabilities. The E-Authentication e-government initiative deployed a prototype e-authentication capability in September. Applications are in the process of being migrated to this service, which will allow for the sharing of credentials across government and allows for secure transactions, electronic signatures, and access controls across government. Potential agencies that will be using this service include DoEd, USDA/National Finance Center, SSA, and GSA. The full capability is expected in September 2003.

Government Information Security Reform - Year Two

Based primarily on agency and IG reports submitted in September, integration of security into agencies' budget processes, and recently updated and submitted IT security plans of action and milestones, OMB has conducted an initial assessment of the Federal government's IT security status. Due to the baseline of agency IT security performance identified last year, we are now in a position to more accurately determine where progress has been made and where problems remain.

The good news is that for the first time the Federal government's IT security program now has a basic set of IT security performance measures and a comprehensive and uniform process for collecting data against those measures. Additionally:

1. More Departments are exercising greater oversight over their bureaus. This year as part of the reporting instructions, agencies were required to report results at the bureau level;

2. At many agencies, program officials, CIOs, and IGs are engaged and working together;

3. IGs have greatly expanded their work beyond financial systems and related programs and their efforts have proved invaluable to the process;

4. More agencies are using their POA&Ms as authoritative management tools to ensure that program and system level IT security weaknesses, once identified, are tracked and corrected; and

5. OMB conditional approval or disapproval of agency IT security programs resulted in senior executives at most agencies paying greater attention to IT security at their agencies.

The bad news is that as we predicted in our previous testimony, the more IT systems that agencies and IG's review, the more security weaknesses they are likely to find. Our initial analysis reveals that while progress has been made, there remain significant weaknesses.

1. Many agencies find themselves faced with the same security weaknesses year after year. They lack system level security plans and certifications. Through the budget process, OMB will assist agencies in prioritizing and reallocating funds to address these problems;

2. Some IGs and CIOs have vastly different views of the state of the agency's security programs. OMB will highlight such discrepancies to agency heads; and

3. Many agencies are not adequately prioritizing their IT investments and therefore are seeking funding

to develop new systems while significant security weaknesses exist in their legacy systems. OMB will assist agencies in reprioritizing their resources through the budget process.

Status of Six Common Government-wide IT Security Weaknesses

In the first annual OMB report to Congress on Federal government information security reform (www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf), OMB identified six common government-wide IT security weaknesses along with steps to overcome those weaknesses. I would like to provide you with an update on efforts related to resolving these weaknesses.

1. Lack of agency senior management attention to IT security. In addition to conditionally approving or disapproving agency IT security programs through private communication between OMB and each agency head, OMB used the President's Management Agenda Scorecard to continue to focus agency attention on serious IT security weaknesses. Through the scorecard OMB and senior agency officials monitor agency progress on a quarterly basis.

2. Non-existent IT security performance measures. As I discussed, OMB developed high-level management performance measures to assist agencies in evaluating their IT security status and the performance of officials charged with implementing specific requirements of the Security Act. Agencies were required to report the results of their security evaluations and their progress implementing their corrective action plans according to these performance measures. To ensure that accountability follows authority, there are measures for both CIOs and program officials. These measures are mandatory and represent the minimum metrics against which agencies must track to measure performance and progress. We encourage agencies to develop additional measures that address their needs.

3. Poor security education and awareness. As discussed above, for one of the Administration's electronic government initiatives, establishing and delivering electronic-training, IT security training options will be added and available to all Federal agencies in December.

4. Failure to fully fund and integrate security into capital planning and investment control. OMB continues to

aggressively address this issue through the budget process, to ensure that adequate security is incorporated directly into and funded over the life cycle of all systems and programs before funding is approved. Through this process agencies can demonstrate explicitly how much they are spending on security and associate that spending with a given level of performance. As a result, Federal agencies will be far better equipped to determine what funding is necessary to achieve improved performance.

Agencies have made improvements in integrating security into new IT investments. However, significant problems remain in regards to ensuring security of legacy systems.

5. Failure to ensure that contractor services are adequately secure. Through the OMB Committee on Executive Branch Information Systems Security, an issue group was created to review this problem and develop recommendations for its resolution, to include addressing how security is handled in contracts themselves. We are working with the Federal Acquisition Regulatory Council to develop for government-wide use a clause to ensure security is addressed as appropriate in contracts.

6. Lack of detecting, reporting, and sharing information on vulnerabilities. Early warning for the entire Federal community starts first with detection by individual agencies, not incident response centers at the FBI, GSA, DOD, or elsewhere. The latter can only know what is reported to them, reporting can only come from detection. It is critical that agencies and their components report all incidents in a timely manner to GSA's Federal Computer Incident Response Center (FedCIRC) and appropriate law enforcement authorities such as the FBI's National Infrastructure Protection Center as required by the Security Act.

GSA recently awarded a contract on patch management. Through this work FedCIRC will be able to disseminate patches to all agencies more effectively. In addition, OMB recently issued guidance to agencies on reporting to FedCIRC, stressing the necessity for accurate and timely reporting while also leveraging an e-business approach that facilitates reporting.

A summary of each agency's security status will be included in the annual OMB report to Congress. We plan on issuing this report in the same timeframe as the President's budget.

While OMB can and will continue to assist agencies with their efforts in addressing their security weaknesses, both the responsibility and ability to fix these weaknesses and others, ultimately lie with agencies. IGs, OMB, and GAO cannot do it for them.

Areas for Additional Attention

OMB, the President's Critical Infrastructure Protection Board, the Federal agencies, and others are also addressing a number of other significant IT security issues.

The Administration strives to ensure that any disruptions to Federal IT systems are infrequent, of minimal duration, manageable, and cause the least damage possible. In that regard, we essentially are addressing two types of threats -- organized (i.e., sophisticated nation states, terrorist, and criminal) and ad hoc (i.e., common hackers of varying levels of sophistication).

Regardless of their level of sophistication (i.e., organized or ad hoc), an attacker can easily exploit numerous vulnerabilities found in today's commercial software products. Some experts estimate that as many as 95% of today's successful attacks exploit these commonly known flaws and most use widely available automated tools to do so. Simple adjustments to out-of-the-box software configurations correct many vulnerabilities and corrective patches are widely available for many others.

We will assure that Federal agencies undertake effective system management practices. This includes tools and training to ensure the timely deployment and continued maintenance of security of IT systems. We are also addressing the out-of-the-box configuration issue. Recently a consortium of Federal agencies and private organizations released security configuration guides for the Windows 2000 operating system. FedCIRC has arranged for download and distribution of the Windows 2000 security testing tool for all Federal civilian agencies.

Countering sophisticated organized threats is far more complex. Many experts consider hostile nation-states and terrorists to pose the greatest threat to the security and reliability of Federal IT systems. This threat is often associated with the threat of physical attack, and could be used to disrupt government coordination and communication in time of emergency.

The development of a government-wide enterprise architecture is a central part of the Administration's IT management and electronic government efforts. Establishment of an architecture for the Federal government will greatly facilitate more rational IT investment decisions and electronic government. Accordingly, the Administration will be able to better prioritize and fund the Federal government's security needs.

Experts agree that it is virtually impossible to ensure perfect security of IT systems. Therefore in addition to constant vigilance on IT security we require agencies to maintain business continuity plans. OMB directed all large agencies to undertake a Project Matrix review to ensure appropriate continuity of operations planning in case of an event that would impact IT infrastructure. Project Matrix was developed by the Critical Infrastructure Assurance Office (CIAO)of the Department of Commerce. A Matrix review identifies the critical assets within an agency, prioritizes them, and then identifies interrelationships with other agencies or the private sector. This is largely a vertical view of agency functions. To ensure that all critical government processes and assets have been identified, once reviews have been completed at each large agency, CIAO and OMB will identify cross-government activities and lines of business for Matrix reviews. In this way the Executive Branch will have identified key needs in both vertical and horizontal continuity of operations.

More and more, individual agencies and other organizations have improved means to protect themselves from more sophisticated attackers. Until recently, commercial firewalls and intrusion detection systems primarily defended only against known attacks. New products filter out actions outside normal use, e.g., those activities that are inconsistent with authorized technical "rules" established by systems administrators. Thus even a previously unknown threat can potentially be stopped. We expect that, as it has in the past, the market will continue to produce solutions to security problems.

Among our high-level challenges is identifying the security gaps between agencies with interconnected lines of business. In addition to Project Matrix and the development of the enterprise architecture as a means to address these potential gaps, we will continue to look for other methods as well, through OMB's Committee on Executive Branch Information Systems Security and the CIO Council.

Conclusion

Again Mr. Chairman, I would like to express the Administration's appreciation for your untiring leadership on IT security.

For the first time, through the reporting requirements of the Security Act and agency POA&Ms, we are able to point to real progress in closing the Federal government's IT security performance gaps. While progress has been made both at the government-wide program level as well as within a number of agencies, serious weaknesses, and in some cases repeating weaknesses remain. Failure to meet basic security requirement such as system plans and certifications leaves us with simply unacceptable risks. Our challenge this year is to dramatically build upon this progress to ensure that the Federal government's IT investments are appropriately secured.

Mr. HORN. And we will now move to the next witness, and then when we finish the witnesses, we will begin the questioning. We are delighted to have the Honorable James B. Lockhart, III, the Deputy Commissioner and Chief Operating Officer of Social Security, Social Security Administration.

Mr. LOCKHART. Thank you, Mr. Chairman and Mr. Lewis. Thank you for inviting me here today to discuss computer security at the Social Security Administration. Commissioner Barnhart and I believe that it is indeed a critical "24x7" issue. We recognize that creating an effective security program is not just a technical issue, but also an issue that demands the attention of top management.

Today I would like to outline the challenges we face and the significant strides our agency has made to further safeguard information security. Our approach to computer security is forward-looking while focusing on continuous monitoring and continuous improvement. The systems challenges we face are substantial. In a typical workday we interact with about 500,000 people through our field offices, telephone network, and Internet services. To handle our workloads we rely on seven mainframe processors based in a national computer center and on more than 100,000 network-connected work stations in over 1,500 locations throughout the country. These computers process more than 35 million transactions a day.

Our Chief Security Officer sets agency policy for information security. That position was recently elevated to report directly to the Chief Information Officer, who reports directly to the Commissioner and myself. The CIO reports to the Commissioner annually on the state of security in SSA, but in reality it's really a regular agenda item at all our executive staff meetings and also at the Executive Internal Control Committee which I chair.

We have made President Bush's management agenda including E-government and a specific security measure part of our new Senior Executive Service Performance System. We have also incorporated a performance measure in our annual performance plan. Systems security has been integrated into our systems development life cycle for more than 15 years. However, in the last year we've begun a number of improvements to ensure that the security program remains responsive to evolving technology and vulnerabilities.

Systems intrusions are one major area of concern. Social Security uses a variety of proactive measures plus individual testing—independent testing and evaluation of security controls to detect and prevent attempted intrusions. For example, we use state-of-the-art software that registers, restricts, and records user access to data. It also determines what function a person can do once they have access to the data. Passwords are changed every 30 days. The software allows Social Security to audit usage and provides a means to investigate allegations of misuse. At least once a month we also scan every work station, telephone, and system platform for compliance.

Social Security's commitment to information security is really shared throughout the whole organization. It is really part of the Social Security culture that is reinforced through training and frequent communications. Frontline employees know to contact the agencywide help desk when a virus or intrusion is suspected. The help desk quickly contacts the "first response group," comprised of both senior management and technical staff, who can rapidly mobilize appropriate resources.

Social Security has a strong critical infrastructure protection process to assure Agency business processing function despite catastrophes. The program includes project matrix reviews, audits risk assessments, remediation plans and related training.

Congress has greatly helped to raise awareness of information security. The Government Information Security Reform Act of 2000 furthered the agenda of systems security by providing for an assessment and reporting mechanism. We completed our annual security self-assessment in September of this year. We actually hired an independent technology consulting firm to look at our self-assessment, and they concurred with our self-rating and were impressed with our security program. Social Security's inspector general's review stated that we met the GISRA requirements and made improvements since last year. However, as we all know, there is always room for further improvement.

In conclusion, Commissioner Barnhart and all of us at Social Security recognize that system security is not a onetime task but an ongoing mission. We know we must be vigilant to ensure that personal records remain secure, taxpayer dollars are protected, and public confidence in Social Security is maintained.

I would also like to thank you, Mr. Chairman, for your work over the years in improving awareness of the importance of not only system security, but also a wide range of program stewardship issues such as financial accounting and reporting debt collection and Y2K. I can assure you that we will continue to work with this subcommittee to help protect the information security of the American people for which we are stewards. I will be happy to answer any questions later.

Mr. HORN. Thank you. And I will hope that there will be excellent people in this, both for the minority and the majority. So thank you. Keep the heat on this subcommittee and vice versa.

Mr. LOCKHART. Yes Mr. Chairman.

[The prepared statement of Mr. Lockhart follows:]

For Release on Delivery

COMPUTER SECURITY: HOW THE AGENCIES RATE

HOUSE COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON
GOVERNMENT EFFICIENCY FINANCIAL
MANAGEMENT AND INTERGOVERNMENTAL RELATIONS

November 19, 2002

SOCIAL SECURITY
USA
ADMINISTRATION

STATEMENT BY
JAMES B. LOCKHART, III
THE DEPUTY COMMISSIONER OF SOCIAL SECURITY

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today in my first appearance before this subcommittee to discuss computer security at the Social Security Administration (SSA). Commissioner Barnhart and I appreciate your interest in systems security, which is a critical issue. She has made service and stewardship key elements of our strategy to effectively administer our programs; systems security is a key stewardship element and it requires continuous improvement, a "24 x 7" mentality.

SSA has always recognized the importance of protecting the privacy of the people we serve and ensuring the integrity and accuracy of the records we keep and the payments we make. The Social Security Board's first regulation, published in 1937, dealt with the confidentiality of SSA records. For more than 65 years, SSA has honored its commitment to the American people to maintain the confidentiality of our records. A natural outgrowth of our emphasis on privacy is a strong commitment to computer security.

We at SSA clearly recognize that the information technology environment is one of constant change due to rapid progress in systems technology and systems security issues that are generated as a result. We continue to be proactive and forward looking in meeting the challenges of this ever-changing environment. We routinely interface with other government agencies and with private and public information technology specialists, to ensure that we stay ahead of developments in this rapidly expanding field.

Building on this strong foundation, I believe we have made significant strides this year in putting in place additional safeguards that will strengthen the security of the information SSA processes and maintains. Today I would like to discuss those safeguards.

Security is a Management Function, Not a Technical Issue

We recognize that creating an effective security program is a management function, and not simply an issue of technical implementation. It demands the attention of our top management. During the course of the last year, Commissioner Barnhart has taken steps to ensure that information security is receiving this level of attention in order to emphasize the importance of making this a priority for every Agency employee. Information security has been made a routine agenda item for the executive staff and has been incorporated into other processes that routinely receive executive-level attention.

Most importantly, information security responsibilities have been realigned to bring the Chief Security Officer under the auspices of SSA's Chief Information Officer (CIO). The Chief Security Officer is responsible for setting Agency policy for information security and for leading and coordinating information technology (IT) physical security policy. The IT budget has also been moved directly under the CIO.

Earlier this month, Commissioner Barnhart announced the appointment of Thomas Hughes as the new CIO for the Agency. Mr. Hughes has an extensive background as a business technology executive and has worked in both the public and private sector including Pricewaterhouse Coopers, and General Dynamics. I am sure he will be a valuable addition to our security team and an excellent CIO.

The Deputy Commissioner of Systems, who also directly reports to us, has 3,000 employees with a total budget of $280 million as well as outside contractor support funded by SSA's IT budget. Another important group, the Office of the Deputy Commissioner for Finance, Assessment and Management, oversees physical and operational systems security.

Systems Challenges

Information technology is intrinsic to our business. The systems challenges at Social Security are large, as we represent a quarter of the federal budget and pay benefits to over 50 million Americans. In a typical workday we interact with almost 500,000 people through our field offices, telephone network and Internet service.

The computing environment at SSA is considerable. SSA relies primarily on seven mainframe processors located in our headquarters' based National Computer Center and a combination of 100,000 plus Microsoft windows NT desktops and UNIX computers for its core information processing. These computers process over 35 million transactions per day and have access to over eleven terabytes of electronic storage. The Agency maintains a global network of communications services that electronically exchanges client information between more than 1500 remote locations and the SSA central processing site.

Externally, the telecommunications environment interfaces with other Government agencies, United States embassies, and State agencies. In addition, SSA has a connection to the Internet to service both internal and external clients.

Improved Security is an Ongoing Process

Systems security is not a new issue to Social Security. We have been safeguarding our records since we began, long before the advent of computers and the technology age. The Agency's policies and procedures have had security integrated into the systems development lifecycle for more than 15 years. However, in the last year SSA has begun implementation of a number of improvements and performance measures in this area to ensure that the security program remains responsive to evolving technologies, conditions, and vulnerabilities.

Our development of systems security is a process geared towards continuous improvements in each facet of the program. We begin by planning for the security needed for each new system and determining how to implement the process. We test the new program thoroughly to determine if it is functioning effectively and providing the required security. We analyze these test results and, if adjustments are needed, make refinements until the system functions as planned. We repeat these steps as our systems are changed and refined.

To make sure that our safeguards are adequate, SSA uses a variety of proactive measures plus independent testing and evaluation of security controls to detect attempted intrusions and prevent them from being successful. We conduct a number of continuous monitoring activities—and I am confident you will understand my reluctance to discuss our specific processes in a public forum. However, we do undergo rigorous evaluation of these processes.

SSA contracts annually to have independent security evaluations completed. In FY 2002, the telecommunications and network infrastructure, all sensitive systems applications, and SSA's web systems received testing in addition to the annual network and systems testing and evaluation performed by SSA's Inspector General with the support from outside experts.

Modern computer security requires the implementation of sophisticated software and control of access to the system. SSA uses state-of-the-art software that carefully restricts any user access to data. Using this software, only persons with a "need to know" to perform a particular job function are approved and granted access to specific kinds of data. Our systems controls not only register and record access, but also determine what functions a person can do once access is authorized. SSA security personnel assign a computer-generated personal identification number and an initial password to persons who are approved for access (the person must change the password every 30 days). This allows SSA to audit and monitor the actions individual employees take when using the system. These same systems provide a means to investigate allegations of misuse and have been crucial in prosecuting employees who misuse their authority.

Additionally, we have implemented processes to scan, at least once a month, every SSA workstation (over 100,000), every telephone, and every systems platform for compliance with Agency standards. I believe that the scope of this program cannot be matched, and our track record in preventing intrusions demonstrates our success in implementing an Enterprise-wide security program that is second to none.

SSA's approach to system security must be forward-looking even as we focus on day-to-day continuous improvement. As an example, four years ago, our auditor listed 4 reportable conditions. Last year we were down to one. In our just completed FY 2002 audit and the auditor indicated that SSA had made notable progress in strengthening its security controls by implementing an effective entity-wide security framework supported by policies and procedures. As recommended, we will continue to implement standard security configurations on our automated platforms and monitor those settings for compliance, using automated techniques where possible. We plan to emphasize our monitoring and reporting program in the coming year. The auditor also noted that contingency planning could be better coordinated among various SSA components; we will improve the level of coordination in the coming year. Over the past several years, SSA has made significant progress in strengthening its security program and will continue to do so. The Agency's Executive Internal Control Committee will monitor progress until all elements of the reportable condition have been addressed and will ensure that resources are made available to support the improvement efforts.

Nurturing a Security Conscious Culture

Of course, SSA's commitment to information security does not stop with top management. While we nurture a security-conscious culture through executive-level attention, we have networks of full-time staff devoted to systems security stationed throughout the Agency. These front-line employees provide day to day oversight and control over our computer software in headquarters and centers for security and integrity in each SSA region.

SSA provides information and reminders to all employees to contact the agency-wide help desk hot line immediately when a virus or intrusion is suspected. This help desk has procedures for quickly contacting the

"First Response Group." This group has senior management members on call in addition to specially trained technical members of the Systems Response team. The Chief Security Officer and a representative of the Office of the Deputy Commissioner for Communications are members of the First Response Group and provide the ability to rapidly mobilize the appropriate resources.

We have tried to put in place the authorities, the personnel, and the software controls to prevent penetration of our systems and to address systems security issues as they surface.

Developing and Implementing Performance Measures

The CIO is required to report to the Commissioner and executive level staff annually on the state of security in SSA, but in reality it is a regular agenda item at executive staff meetings and the Executive Internal Control Committee, which I chair. And the way we measure the effectiveness of our security is through performance measures that provide quantitative feedback. These measures allow us to identify and focus on areas that most need attention. For example, the CIO performance measure for FY 03 is that no more than 200 workstations, out of over 100,000 workstations would be adversely affected by any security incident, such as a virus. In FY 04, the measure is for no more than 100 workstations affected.

In addition, we have made President Bush's Management Agenda initiatives, including e-government, performance measures in the Performance Plan for all members of the Senior Executive Service. We also have a specific measure to: "Safeguard[s] the workforce, infrastructure, and workplace to prepare for and mitigate negative consequences."

SSA has established specific measures of performance to ensure that program officials have assessed the risk to operations and assets, assigned the appropriate level of security to protect such operations, and maintain up-to-date security plans. To ensure this happens, all sensitive systems are reviewed and recertified on an annual basis by the System Managers and an inter-component Sensitive System Review Board. We have established other performance measures to ensure that security controls and techniques are tested and evaluated, and monitor whether the performance measures have been met.

Deputy Commissioners are responsible for ensuring that each sensitive system has an up- to-date security certification. A risk analysis and recertification that each sensitive system has adequate safeguards is required annually.

Critical Infrastructure Protection Process

Mr. Chairman, the tragic events of last September 11 stand as an unforgettable reminder that we need to be prepared for catastrophic events that may threaten not only our systems security but our physical security and our ability to conduct our business with the public.

SSA has in place a strong management control program to assure Agency business processes function as intended. The Critical Infrastructure Protection Process (CIP) creates a comprehensive Agency-wide approach addressing physical security, continuity of operations, and information systems security. The CIP process systematically identifies critical functions and the assets that support those functions.

"he program includes recurring reviews, audits, risk assessments, remediation plans, related training and -awareness, and other checks and balances designed to protect SSA's normal business processes in even the most extraordinary circumstances. Using Project Matrix, 7 of 8 critical assets Step 1 reviews have been completed. By the end of this year we expect to complete the remaining Step 1 review and half of the Step 2 reviews.

Congress Has Helped

Congress has helped to raise the level of awareness of the importance of information security with the enactment of the Computer Security Act of 1987, which directed all Federal agencies to establish a designated Agency-level security official and laid the framework for development of formal security programs.

The Government Information Security Reform Act of 2000 (GISRA) furthered the agenda of systems security by providing for an assessment and reporting mechanism that ensures that security programs continue to improve.

SSA completed its annual security self-assessment for FY 2002, as required by GISRA, this September. We also engaged a major technology consulting firm to conduct interviews and documentation reviews and independently determine the validity of our assessment. I am pleased to report that they concurred with the self-rating of SSA staff and were impressed with the administrative quality, organizational integration, and technical strength of SSA's security program. Also, SSA's Inspector General reviews the annual security self-assessment using our external auditing firm. Their report stated that we met the GISRA requirements, and 'ade improvements since last year. However, as they stated, and as external consultants have said, there are always areas for improvement.

Finally, I would like to thank you, Mr. Chairman for your work over the years in improving awareness of the importance of not only systems security but also a wide range of program stewardship issues such as financial accounting and reporting, debt collection, and Y2K. Your work and the work of all the members of the subcommittee helps assure the American people that they can continue to rely on SSA's stewardship of our programs and that our systems maintain the privacy of the information we hold.

Conclusion

In conclusion, Mr. Chairman, Commissioner Barnhart and I, and all other employees of the Social Security Administration, recognize that systems security is not a one-time task to be accomplished, but an ongoing mission. It is a critical component of providing service and stewardship to the American people. We know we cannot rest on past practice, but must be vigilant in every way we can to assure that these personal records remain secure, taxpayer dollars are protected, and public confidence in Social Security is maintained.

I can assure you that we will continue to work with the Subcommittee to assure the American people that we are doing all we can to maintain the security of our computer operations. I will be happy to answer any questions you may have.

Mr. HORN. And we now have a longtime friend of this committee, the Honorable Kenneth M. Mead, Inspector General, Department of Transportation.

Mr. MEAD. Thank you, Mr. Chairman, Mr. Lewis. Like my colleagues and Mr. Lewis, I would like to start by just saying thank you for so many things over the years. This hearing is—I suppose the words almost certainly would apply here—one of the last hearings that you'll be conducting in this capacity. And you've truly been a champion of good government. I think most recently—the successful transition to Y2K was a triumph of the oversight practices of this committee and your stewardship—but it's the full range of management issues, that inspector general community will miss you for.

I mentioned Y2K. Actually, computer security has a lot of similarities with the Y2K experience. If you stop and think about it, Y2K involved a process where you first had to inventory your systems. You had to identify the vulnerabilities. Then you had to do a cost-effective risk analysis of what holes needed to be plugged and you had to set priorities. A big difference, of course, is that in Y2K we had a date certain to meet. No waivers from anybody. It was bound to happen. Those were the marching orders.

Here the date is a little less fuzzy, but I think we need to move forward with the same sense of vigor because of the importance of the area.

I'd like to summarize where DOT has been, what progress has been made, and what it needs to do to secure its critical systems. And the bulk of my testimony is based on the report we recently issued under GISRA. OMB has it. You have it. The Secretary has it. And we're pleased with the Departments' response. DOT's information security program remains a material weakness, as reported last year, and we're going to recommend that it be reported as such again this year.

I must say that under Secretary Mineta's leadership, DOT has made a strong commitment for improvement and there is noticeable progress that I can specify, but they have a long way to go. A notable example of the progress has been that DOT significantly enhanced defense against intrusions from the Internet. FAA upgraded increased background collection on its employees.

But there are six areas that DOT needs to focus on and here they are: First and foremost, as in most things, establish leadership. DOT does not have a CIO, Chief Information Officer. And, in fact, in the 6 years since the Clinger-Cohen Act was passed, we've had a CIO for 18 months of that period, and we don't have one now. I should say that it's not for want of active recruiting. But we need one. And, Mr. Chairman, it's not only a case of just having a CIO, someone with that title. The DOT CIO Office, in our judgment, does not have sufficient authority or controls over the operating divisions' information technology budgets or performance. You know, DOT is set up—we have about 9 or 10 agencies: FAA, Coast Guard, the Federal Highway Administration, so forth and so on. But the operating divisions generally have not in the past been held accountable to answer to the CIO. This will be evidenced in several of the other points I'm going to illustrate here.

A second area is securing computer systems against unauthorized intrusions. Several years ago when we reported to this committee that DOT did not have firewall security. Intruders could easily gain access to DOT computers systems from the Internet. Two years ago, we testified that the firewall security was not strong enough and there were unsecured "back doors" to access DOT computers. Since then, DOT has enhanced its firewall security against unauthorized intrusions from the Internet which are referred to as the "front door." But, despite repeated directives from the Agency's CIO office, there are still a significant number of unsecured "back doors." What are back doors? Back doors are dial-up modems. They are non-DOT computers that are connected to those of DOT's, in many cases, by the hundreds of contractors that DOT has. We think that's a significant risk area.

Third, reporting cyber incidents. DOT needs to do a better job in analyzing reporting major cyber incidents. Last year they reported 25,000 incidents. But most of those were not analyzed or stratified for degree of seriousness. And most of them, my guess is, were innocent acts of somebody misusing a password or whatever. We also found, though, that 3 of 10 major incidents we had went unreported to the Federal Computer Incident Response Center. We think that needs to be strengthened.

Fourth, protect E-government services. DOT needs to better protect its public Web sites from being attacked. In our audit work, we identified 450-odd vulnerabilities throughout DOT. Forty percent of them were at FAA, and the Federal Highway Administration had 113 of them. Of the 450-odd vulnerabilities, Mr. Chairman, we would rank about 80 of them as being very serious, meaning that they could allow attackers to take control over DOT Web sites. DOT, I should note, promptly corrected the vulnerabilities we identified.

Fifth area, check contractors' employees background. DOT still needs to do more in this area. I'm happy to report that FAA has made progress. I believe it was at a hearing before this and a couple of other congressional committees where this was a major problem 3 years ago. Our tests now indicate that about 84 percent of FAA contractor employees have received background checks versus just 23 percent 2 years ago. But still the delta between that 84 percent and 100 percent is too significant, in my view. Unfortunately, other DOT agencies have not made as much progress and their compliance rate rose only from 13 percent to 14 percent.

And, finally, a major task is to get all DOT's 561 mission-critical systems certified for adequate security. The current date for doing that is set at December 2005. This challenge is particularly similar to Y2K. Right now, we have completed the security assessment—not we, the DOT, of 123 of 561 systems. They have a long way to go. And I'm a little concerned about the date of December 2005 being several years away. I'd like to see this process be accelerated but it's going to require top management commitment to put the pressure on.

And finally, Mr. Chairman, I'd like to say a word about the role for inspector general and GAO. And I think this is alluded to in Mr. Forman's written statement. I'm concerned that too much reliance is being placed on the inspector generals and GAO to identify vulnerabilities. As I noted, we identified 450-odd of them. Those were plugged when we identified them. But you don't want to rely on your inspector generals or GAO to identify all the vulnerabilities. Inspector generals are fairly small operations. We're supposed to audit. We are not in the business of running the security program. I'm pleased to report that I think under Secretary Mineta's leadership this is beginning to change at DOT, but it needs to change in a much larger way. Thank you.

Mr. HORN. Thank you, and we appreciate the thoughts you have there and we'll get to that a little later.

[The prepared statement of Mr. Taylor follows:]

STATEMENT OF
EUGENE K. TAYLOR, JR., ACTING CHIEF INFORMATION OFFICER
US DEPARTMENT OF TRANSPORTATION
BEFORE THE
COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON GOVERNMENT EFFICIENCY,
FINANCIAL MANAGEMENT, AND INTERGOVERNMENTAL RELATIONS
U.S. HOUSE OF REPRESENTATIVES
November 19, 2002

Mr. Chairman and Members of the Committee. On behalf of the US Department of Transportation (US DOT) let me thank you for this opportunity to discuss our IT Security Program. For the purposes of today's hearing, I will provide the Committee with an overview of US DOT's Information Technology (IT) Security Program, our progress in FY2002, and our plans for improvements in Fiscal Year 2003. I would like to first acknowledge the role you have played in the last decade on IT Security issues. Through your attention to this issue we have all witnessed a substantial increase in attention and efforts to improve visibility of the IT Security problem. While we still have some challenges to overcome within the US Department of Transportation, I am pleased to report today that we are demonstrating progress. We believe we now have a sound cyber security strategy to guide the department and to prioritize our activities. We also believe that we have made solid progress during 2002. That said, we are fully aware that this "Rome" will not be built in a day. We have an aggressive program for 2003, and we are laying the groundwork for efforts that will take additional years and resources to fully address the cyber security challenge facing our department and our nation. Therefore, I am pleased to report that we are demonstrating progress due in large part to your leadership

Background

The US Department of Transportation (US DOT), based on the leadership and commitment of Secretary Mineta, has made significant efforts to improve our IT Security program over the past several years. The enactment of the Government Information Security Reform Act of 2000, along with the events of September 11, 2001, have resulted in a renewed priority and focus on this program. In particular, GISRA has provided insightful guidance and a performance-based reporting process that has assisted us in making IT Security a top priority in the Department. In 2001, US DOT demonstrated a commitment to the IT Security program by hiring a Senior Executive, selected from a pool of over 60 applicants representing IT Security experts in both Government and Industry, to lead the US DOT IT Security Program. She has an extensive background in IT Security. She has served as a US Army Military Intelligence Officer, as a Director and Vice-President in various IT Security consulting firms, and as a Senior Manager with Ernst & Young LLP, and has over 16 years of experience in designing IT Security programs and solutions for both Government agencies and financial services institutions. In conjunction with her hiring, the Department embarked on a thorough assessment, using the NIST 800-26 standards, of the IT security posture of our 15 Operating Administrations (OA) [1] to identify and assess our IT Security risks as a part of both the FY2001 and the FY2002 GISRA process. As you know, the breadth of our Information Technology portfolio is vast, consisting of thousands of systems supporting mission

[1] For the purposes of this document, the term "Operating Administration (OA)" refers to the following 15 organizations, including the Office of the Secretary (OST), the Bureau of Transportation Statistics (BTS), the Surface Transportation Board (STB), the Transportation Administrative Service Center (TASC); and then 11 OAs, i.e., Federal Aviation Administration (FAA), Federal Highway Administration (FHWA), Federal Motor Carrier Safety Administration (FMCSA), Federal Railroad Administration (FRA), Federal Transit Administration (FTA), Maritime Administration (MARAD), National Highway Traffic Safety Administration (NHTSA), Research and Special Programs Administration (RSPA), Saint Lawrence Seaway Development Corporation (SLSDC),

critical safety, security, and economic mobility business operations. Consequently, this assessment was a substantial accomplishment for the Department, and allowed us to recognize a baseline from which to begin implementing change. Based on the weaknesses identified during these reviews by the US DOT Office of the Chief Information Officer (OCIO), the Operating Administrations, the US DOT Inspector General, and the General Accounting Office, and feedback from OMB, US DOT developed and gained executive approval to execute an enterprise-wide, comprehensive FY 2002 Agency Security Plan that was embraced by all Operating Administrations. This was the cornerstone of our strategy to improve IT Security – ensuring that the previously divergent Operating Administrations collaborated to jointly develop and execute this plan. Within the department, our Operating Administrations philosophically converged and committed to a shared vision and set of goals for improving the IT Security program in FY2002. In fact, the Federal Aviation Administration (FAA) assumed a key leadership role on behalf of the Department by leading an IT Security subcommittee under the Department's CIO Council to establish these goals. Additionally, the DOT OCIO and the Inspector General formed a collaborative relationship that contributed to identifying the weaknesses in our program, and establishing the strategy for improvements. The consensus goals for the FY 2002 US DOT IT Security Program were to: Increase senior executive visibility and commitment to the IT Security program; Establish a comprehensive Performance Measurement Program that mapped IT security program performance to the President's Management Agenda; Conduct specialized training for personnel performing IT Security duties; Integrate IT Security into the Capital Planning and Investment Control (CPIC) process;

Establish a comprehensive incident reporting program; and Focus on implementing network and perimeter security controls. The Department has accomplished the following in FY 2002 as a result of executing this plan, which was driven by accomplishing the first goal: gaining a renewed executive commitment to the US DOT IT Security Program from the Secretary, his staff, and the Heads of our Operating Administrations. The Secretary personally designated May, 2002 as the Department's First Annual Computer Security Month, established awards for achievements in IT Security for individuals, and supported attendance at a scheduled awareness event for the executive staff. The second goal accomplished by the US DOT was the development of a comprehensive IT Security Performance Measurement (IT SPM) program to identify and track quantifiable results related to key IT security metrics. The results from our FY2001 and FY2002 GISRA assessments served as the baseline from which progress was measured. The results of this program indicated that in FY2002, the Department made noteworthy improvement in reducing IT security program related weaknesses and by reducing vulnerabilities, and thus risks, in our primary demilitarized zone (DMZ). Our third goal was to institute a robust training and awareness program, focused on developing and providing specialized training to IT security personnel. Based on this program, US DOT provided awareness training to the majority of our employees, and provided specialized training in certification and accreditation (C&A) and network security to the majority of the Agency-level Information Systems Security Officers (ISSO). Additionally, the program provided a specialized, hands-on 5-day training course to more than 74 departmental systems administrators. Our fourth goal was to develop and began implementing a comprehensive policy for integrating IT security into the CPIC process. The policy, effective June 2002, prescribed that Agency ISSOs participate as members of the CPIC review board; the policy also outlined the requirements for IT security in each phase of the CPIC and the system development life cycle, and it stipulated a methodology for estimating security costs. The implementation of this policy began with the FY 2004 budget process, where all applicable programs incorporated security percentages. Our fifth goal was to develop and execute an Incident Reporting Policy Memorandum and begin reporting incidents on a weekly basis to the Federal Computer Incident Response Center (FedCIRC), the National Infrastructure Protection Center (NIPC) and other law enforcement agencies as required. In addition, the Department continued to implement intrusion detection systems (IDS) at critical access points throughout the US DOT backbone and on the local area network of the National Highway Traffic Safety Administration (NHTSA), Research and Special Programs Administration (RSPA) and the FAA. Although the focus in FY2002 was network/perimeter security, DOT/FAA continues to certify and authorize mission critical systems deployment while addressing these new, complex cyber threats at the electronic boundary of the DOT enterprise. The Department published comprehensive network security guidelines and began a Web server vulnerability testing program in the US DOT DMZ. Based on this program, vulnerabilities decreased by a large percentage. In addition, the Department continuously looked for opportunities to leverage a "buy once, service many" philosophy. For example, the US DOT established a contract for an enterprise-wide vulnerability scanning tool that was made available to all Operating Administrations. This contract was the result of an FAA product testing effort, and provided all Operating Administrations with an effective, low cost, cross cutting solution for vulnerability identification, management and risk tracking, and remediation. Although we made great progress in FY2002, US DOT also acknowledges several areas as opportunities for continuous improvement in the IT Security Program. IT funding must be prioritized to ensure that IT security weaknesses are appropriately funded. In addition, these weaknesses also illustrate a requirement to focus our attention from improving perimeter and network security to a more system-centric approach in the FY 2003 Agency Security Plan. Increased emphasis needs to be placed on program integration and resulting system-level reporting and control effectiveness, including the development of an improved system inventory methodology, Certification and Accreditation guidance, and improved levels of reviews of mission critical IT systems. Although process improvements have been made in vulnerability testing, US DOT will be expanding this program to include all Web servers and to internal systems in the upcoming year, and to conduct periodic compliance reviews. External connections, including dial-up, need to be thoroughly reviewed and secured, and contracts must be modified to specify that Application Service Providers and other partners must meet US DOT personnel and IT security policy and guidance prior to connecting to or hosting a US DOT site. Although there have been improvements in US DOT's Incident Reporting and Response Program, additional guidelines will be implemented to ensure consistency in the process. Based on the identification of the weaknesses indicated above, US DOT has established the following goals and objectives for FY 2003–2004. US DOT plans to develop and implement a standard methodology for IT system inventory and implement an established system review process. Additionally, by the end of FY 2003, US DOT plans to have completed system reviews for an increased number of US DOT mission critical IT systems. US DOT is also implementing consistent incident detection and reporting capabilities Department-wide, and through the FAA is collaborating with FedCIRC and other leading agencies on methods to more rapidly share incident and cyber-threat data. US DOT will also be designing a common access control architecture to improve system-level access controls in collaboration with the government-wide e-Authentication initiative. With the adoption of the enterprise-wide tool, vulnerability testing and reporting will be expanded to a larger percentage of US DOT IT systems. US DOT is also planning on completing integration with the Enterprise Architecture process and incorporating process improvements into the CPIC based on lessons learned from the FY 2004 budget process. US DOT will continue to participate in Project Matrix and the upcoming FedCIRC patch management system. The Department also looks forward to continued participation in the Executive Branch Information Systems Security Committee (EBISS) and the e-Authentication initiative, and in other opportunities where the Federal Government can obtain performance and cost efficiencies through collaborative projects. While many improvements have been made in our IT Security program over the past year, the fact is that systemic improvements will only occur if IT resources for security are appropriately prioritized and integrated into systems and programs. The department acknowledges that effective management, IT capital planning integration, strategic planning, and identification of security gaps is the baseline for establishing a solid IT Security program. I trust that you will derive from my remarks an understanding of the efforts the US DOT has taken to improve our IT Security program, and the commitment of Secretary Mineta to continue to focus on this critical program. We appreciate your leadership, and that of the Committee, for helping us achieve our goals and allowing us to share information that we feel is crucial to the protection of our Department's information technology resources.

Mr. HORN. We now have Richard D. Pethia, and he is the Director of the CERT Coordination Center of Carnegie Mellon, and you've been very helpful to this subcommittee over the last decade and a half. And you might want to put on the record, what does CERT mean? And we would be glad to hear from you.

Mr. PETHIA. Thank you. Mr. Chairman and members of the subcommittee, thank you for the opportunity to testify on computer security issues. And Mr. Chairman, thank you especially for helping us all focus on this important IT-related topic.

My perspective comes from the work that we do at the CERT, the Computer Emergency Response Team, where since 1988 we have handled over a 170,000 separate computer security incidents and catalogued more than 8,000 computer vulnerabilities. During that time, the Internet has changed dramatically and computers have become such an integral part of American government and business that computer-related risks cannot be separated from national defense, general safety, health business and privacy risk. Valuable government and business assets along with personal information, critical services, are now at risk over the Internet. Our increasing dependency on these network systems is being matched by increasing the number of attacks aimed at those systems.

The CERT Coordination Center alone, one of only over 200 incident response teams globally, has seen a dramatic increase in the number of incidents reported over just the last 4 years, from 3,700 in 1998 to over 53,000 in 2001; and at the current reporting rates, 2002 will top 100,000 separate incidents. These attacks are aimed at systems across government and industry, and have led to loss and compromise of sensitive data, loss of productivity, system damage, financial loss, and loss of reputation and customer confidence. Virus and worm attacks alone have resulted in hundreds of millions of dollars of loss in just the last 12 months.

Most threatening of all is the link between cyber space and physical space. Supervisory control and data acquisition systems are used to control power grids, water treatment and distribution systems, oil and chemical refineries, and other physical systems. Increasingly, these control systems are being connected to communications links and networks to reduce operational costs by supporting remote maintenance and remote control functions. These systems are potential targets of individuals bent on causing massive disruption and physical damage. This is not theory. Actual attacks have caused major operational problems in Australia, for example, where attacks against sewage plants have led to the release of hundreds of thousands of gallons of sewage sludge.

The Internet has become a virtual breeding ground for attackers. Intruders share information about vulnerable sites, vulnerabilities in the technology and attack tools. Internet attacks are difficult to trace. The protocols make it easy for attackers to hide their identity and location on the network. The number of cyber attackers that have been identified and prosecuted is minuscule compared to the number of security incidents that are reported on an ongoing basis.

Our systems are vulnerable. Last year we received 2,400 vulnerability reports, reports of weaknesses in pieces of software, and we expect to receive over 4,300 reports by the end of this year. These vulnerabilities are caused by security weak design and development practices. With this number of vulnerabilities, fixing vulnerable systems is deemed difficult. System and network administrators are in a hard spot. It is often months or years before patches are implemented on the vulnerable computers, and we often receive reports even years after the fact of attacks of vulnerabilities that have been in fact known for 2 or 3 years.

And at the same time, the attack technology is advancing. Today, intruders use worm technology and other automated methods to reach tens of thousands of computers in minutes, where it once took weeks or months.

Working our way out of this vulnerable position will require a multipronged approach:

First, higher quality products. Good software engineering practices can dramatically improve our ability to withstand attacks. The solution is going to require a combination of virus-proof software, reducing implementation errors by at least two orders of magnitude over today's levels, and requiring that vendors ship products with high security default configurations. We encourage the government to use its buying power to demand such higher-quality software.

Acquisition processes must place more emphasis on security characteristics, and we suggest using code integrity clauses that hold vendors more accountable for defects in their release products. Acquisition professionals should be trained in current government security regulations and policies, but also in the fundamentals of security concepts and architecture. It's important that these people understand not only how to work within the letter of the law but also the spirit of the law to get the quality of software that we require in our national systems.

Also needed is wider adoption of security practices. Senior management attention here is important. Senior management must increase its involvement with visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements. For the long term, research is also essential to seek fundamental technological solutions and preventive approaches. Needed in the long term is a unified and integrated framework for all information assurance analysis, rigorous methods to quantifiably assess and manage risks, quantitative techniques to determine the cost/benefit of risk mitigation strategies, and simulation tools to analyze the cascade effects of attacks, accidents, and failures across interdependent systems.

The Nation as a whole requires more qualified technical specialists. Government scholarship programs that have started are a good step in the right direction, but they need to be expanded over the next 5 years to build the university infrastructure we need for the long-term development of trained security professionals.

Also needed is more awareness and training for all Internet security users, with special emphasis paid to students in grade schools who can begin to understand the ethics of use of these wide area networks as they understand ethics in other kinds of situations.

In conclusion, security incidents are almost doubling each year, and attack technology will continue to evolve to create attacks that are even more virulent and damaging. Solutions are not simple but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. We can make significant progress by making changes in software design and development practices, giving more management support to risk management activities, increasing the number of trained system managers and administrators, and improving the level of knowledge of all users, and increasing research under secure and survivable systems. Thank you.

[The prepared statement of Mr. Pethia follows:]

Information Technology—
Essential But Vulnerable:
Internet Security Trends

Testimony of Richard D. Pethia
Director, CERT® Centers
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Before the
House Committee on Government Reform
Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations

November 19, 2002

Introduction

Mr. Chairman and Members of the Subcommittee:
My name is Rich Pethia. I am the director of the CERT® Centers. Thank you for the opportunity to testify on computer security issues that affect the government. Today I will discuss the vulnerability of information technology on the Internet, including information about recent security trends, and steps I believe we must take to better protect our critical systems from future attacks.

My perspective comes from the work we do at the CERT Centers, which are part of the Survivable Systems Initiative of the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. We have 14 years of experience with computer and network security. The CERT Coordination Center (CERT/CC) was established in 1988, after an Internet "worm" became the first Internet security incident to make headline news, acting as a wake-up call for network security. In response, the CERT/CC was established at the SEI. The center was activated in just two weeks, and we have worked hard to maintain our ability to react quickly. The CERT/CC staff has handled well over 173,000 incidents and cataloged more than 8,000 computer vulnerabilities.

The CERT Analysis Center, established just two years ago, addresses the threat posed by rapidly evolving, technologically advanced forms of cyber attacks. Working with sponsors and associates, the CERT Analysis Center collects and analyzes information assurance data to develop detection and mitigation strategies that provide high-leverage solutions to information assurance problems, including countermeasures for new vulnerabilities and emerging threats. The ultimate goal of this work is to predict technologically sophisticated cyber attacks and develop defensive measures to protect against them before they are launched. The CERT Analysis Center builds upon the work of the CERT Coordination Center.

The CERT Centers are now recognized by both government and industry as a neutral, authoritative source of data and expertise on information assurance. In addition to handling reports of computer security breaches and vulnerabilities in network-related technology, we identify preventive security practices, conduct research, and provide training to system administrators, managers, and incident response teams. More details about our work are attached to the end of this testimony (see *Survivable Systems Initiative*).

The Growing Risk

Government, commercial, and educational organizations depend on computers to such an extent that day-to-day operations are significantly hindered when the computers are "down." Currently, many of the day-to-day operations depend upon connections to the Internet and other interconnected networks, and new connections are continuously being made. The Internet Domain Survey (http://www.isc.org/ds/) reports that the Internet grew from 109 million computers in January 2001 to more than 147 million in January 2002.

Computers have become such an integral part of American government and business that computer-related risks cannot be separated from national defense, general safety, health, business, and privacy risks. Valuable government and business assets, along with critical services, are now at risk over the Internet and other information infrastructures. For example, citizen and personnel information may be exposed to intruders. Public safety services, health services, defense operations, and commerce conducted over the networks can be disrupted. Financial data, intellectual property, and strategic plans may be at risk. The widespread use of databases threatens the privacy of individuals. Increased use of computers in safety-critical applications, including the storage and processing of medical records data, increases the chance that accidents or attacks on computer systems can cost people their lives.

Today there is rapid movement toward increased use of interconnected networks for a broad range of activities, including defense, commerce, education, entertainment, operation of government, and supporting the delivery of safety, health, and other human services. Although this trend promises many benefits, it also poses many risks. Techniques that have worked in the past for securing systems are not effective in the current world of networks without well-defined boundaries, mobile computing, distributed applications, and dynamic computing. It is easy to exploit the many security holes in our networks and in the software commonly used in conjunction with it; and it is easy to hide the true origin and identity of the people doing the exploiting. Many of our information systems are easily accessible to anyone with a computer and a network connection. Individuals and organizations worldwide can reach any point on the network without regard to national or geographic boundaries.

The Growing Threat

Our increasing dependency on these networked systems is being matched by an increase in the number of attacks aimed at these systems. The CERT Coordination Center alone, one of more than 200 computer security incident response teams globally, has seen a dramatic increase in incidents reported over the last four years: from 3,734 incidents reported in 1998 to over 52,000 incidents reported in 2001. At current rates, the number of incident reports for 2002 is estimated to top 97,000. Other teams are reporting similar growth in the number of incidents reported to them.

These attacks have been aimed at systems across government and industry and have led to loss and compromise of sensitive data, system damage, lost productivity because of system down time, financial loss, and loss of reputation and customer confidence. Virus and worm attacks alone have resulted in hundreds of millions of dollars of loss in just the last twelve months.

While many of the attacks on the Internet today could be classified as nuisance activities, there is growing evidence that criminals and terrorists view the Internet as a tool to reach their goals.

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted while also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiple benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography and pedophile rings, but also drug trafficking and criminal organizations that are more concerned about exploitation than the kind of disruption that is the focus of the more general intruder community.

Cyber Space and Physical Space Are One

Most threatening of all is the link between cyber space and physical space. Supervisory control and data acquisition (SCADA) systems and other forms of networked computer systems have for years been used to control power grids, gas and oil distribution pipelines, water treatment and distribution systems, hydroelectric and flood control dams, oil and chemical refineries, and other physical systems. Increasingly, these control systems are being connected to communications links and networks to reduce operational costs by supporting remote maintenance, remote control, and remote update functions. These computer-controlled and network-connected systems are potential targets of individuals bent on causing massive disruption and physical damage.

This is not just theory; actual attacks have caused major operational problems. Attacks against wastewater treatment systems in Australia, for example, led to the release of hundreds of thousands of gallons of sludge.

A recent article in the *Washington Post*[1] reports that our growing dependence on computer-controlled and network-connected infrastructures—and the damage that could result from cyber attacks against those infrastructures—has not gone unnoticed by terrorist organizations. As the article reports: "...U.S. investigators have found evidence in the logs that mark a browser's path through the Internet that al Queda operators spent time on sites that offer software and programming instructions for the digital switches that run power, water, transport, and communications grids." And "...al Queda prisoners have described intentions, in general terms, to use those tools."

The Internet is Attractive to Attackers

Compared with other critical infrastructures, the Internet seems to be a virtual breeding ground for attackers. There is (loosely) organized attack tool development in the intruder community, with only a few months elapsing between "beta" software and active use in attacks. Moreover, intruders take an open-source approach to development. There are parallels with open system development: many developers and a large, reusable code base.

Intruders are also developing techniques to harness the power of hundreds of thousands of vulnerable systems on the Internet. Using what are called distributed-system attack tools, intruders can harness a large number of compromised computers simultaneously, focusing all of them to attack one or more victim computers or networks. In addition, sophisticated developers of intruder programs package their tools into user-friendly forms and take advantage of the Internet to make them widely available. As a result, even technically unsophisticated intruders can use them to cause serious damage.

Unfortunately, Internet attacks in general, and denial-of-service attacks in particular, remain easy to accomplish, hard to trace, and a low risk to the attacker.

Internet Attacks Are Easy

Both the nature of Internet users and the nature of the Internet itself make attacks easy. Internet users place unwarranted trust in the network. It is common for sites to be unaware of the amount of trust they actually place in the infrastructure of the Internet and its protocols. The Internet was originally designed for robustness from attacks or events that were external to the Internet infrastructure; that is, physical attacks against the underlying physical wires and computers that make up the system. The Internet was not designed to withstand internal attacks—attacks by people who are part of the network; and now that the Internet has grown to encompass so many sites, hundreds of millions of users are effectively inside the network.

The Internet is primarily based on protocols (rules and conventions) for sharing electronically stored information, and a break-in is not physical as it would be, for example, in the case of a power plant. It is one thing to be able to break into a power plant, cause some damage, then escape. But if a power plant were like the Internet, intruders would be able to stay inside the plant undetected for weeks. They would come out at night to wander through the plant, dodging a few

[1] "Terrorists at Threshold of Using Internet as Tool of Bloodshed, Experts Say," *Washington Post,* 27 June 2002.

guards and browsing through offices for sensitive information. They would hitch a ride on the plant's vehicles to gain access to other plants, cloning themselves if they wished to be in both places at once. The openness of the network and the availability of easy access provide intruders with many paths to successful attacks.

Internet Attacks Are Difficult to Trace

Internet protocols make it easy for attackers hide their identity and location on the network. Information on the Internet is transmitted in packets, each containing information about the origin and destination—senders provide their return address, but they can lie about it. Most of the Internet is designed to merely forward packets one step closer to their destination with no attempt to make a record of their source. Unlike traditional paper mail, there is not even a postmark to indicate generally where a packet originated. It requires close cooperation among sites and up-to-date equipment to trace malicious packets during an attack.

Moreover, the Internet is designed to allow packets to flow easily across geographical, administrative, and political boundaries. Consequently, cooperation in tracing a single attack may involve multiple organizations and jurisdictions, most of which are not directly affected by the attack and may have little incentive to invest time and resources in the effort.

This means that it is easy for an adversary to use a foreign site to launch attacks against U.S. systems. The attacker enjoys the added safety of the need for international cooperation in order to trace the attack, compounded by impediments to legal investigations. It is common to see U.S.-based attackers gain this safety by first breaking into one or more foreign sites before coming back to attack their desired target in the U.S.

Internet Attacks Are Low Risk

Failed attempts to break into physical infrastructures involve a number of federal offenses; such events have a long history of successful prosecutions. This is not the case for Internet intrusions. Because attacks against the Internet typically do not require the attacker to be physically present at the site of the attack, the risk of being identified is reduced. In addition, it is not always clear when certain events should be cause for alarm. For example, what appear to be probes and unsuccessful attacks may actually be the legitimate activity of network managers checking the security of their systems. Even in cases where organizations monitor their systems for illegitimate activity, which occurs in only a small minority of Internet-connected sites, real break-ins often go undetected because it is difficult to identify illegitimate activity. In the case of cross-site scripting, web users trigger malicious code without even knowing they have done so, and web sites can unknowingly pass the code along. Finally, as mentioned earlier, because intruders cross multiple geographical and legal domains, there are difficult legal issues involved in pursuing and prosecuting them.

Our Systems are Vulnerable

Last year, the CERT/CC received 2,437 vulnerability reports, more than double the number of the previous year. In the first three quarters of 2002, we have already received 3,222 reports and expect over 4,300 reports by the end of this year. These vulnerabilities are caused by software designs that do not adequately protect Internet-connected systems and by development practices that do not focus sufficiently on eliminating implementation flaws that result in security problems.

There is little evidence of movement toward improvement in the security of most products; software developers do not devote enough effort to applying lessons learned about the causes of vulnerabilities. We continue to see the same types of vulnerabilities in newer versions of products that we saw in earlier versions. Technology evolves so rapidly that vendors concentrate on time to market, often minimizing that time by placing a low priority on the security of their products. Until customers demand products that are more secure or there are changes in the way legal and liability issues are handled, the situation is unlikely to change.

Additional vulnerabilities come from the difficulty of securely configuring operating systems and applications software packages. These products are often shipped to customers with security features disabled, forcing the technology user to go through the difficult and error-prone process of properly enabling the security features they need. While the current practices allow the user to more quickly use the product and reduce the number of calls to the product vendor's service center when a product is released, it results in many Internet-connected systems that are misconfigured from a security standpoint.

Attack Technology is Advancing

CERT/CC experience shows that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop exploit scripts for vulnerabilities discovered in products. They then use these scripts to compromise computers and, as mentioned earlier, share these scripts so that more attackers can use them. These scripts are combined with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

These new attack technologies are causing damage more quickly than those created in the past. The Code Red worm spread around the world faster in 2001 than the so-called Morris worm moved through U.S. computers in 1988, and faster than the Melissa virus in 1999. With the Code Red worm, there were days between first identification and widespread damage. Just months later, the Nimda worm caused serious damage within an hour of the first report of infection.

In the past, intruders found vulnerable computers by scanning each computer individually, in effect limiting the number of computers that could be compromised in a short period of time. Now intruders use worm technology to achieve exponential growth in the number of computers scanned and compromised. They can now reach tens of thousands of computers in minutes where it once took weeks or months.

This fast exploitation limits the time security experts like those at the CERT/CC have to analyze the problem and warn the Internet community. Likewise, system administrators and users have little time to protect their systems.

Fixing Vulnerable Systems is Difficult

With an estimated 4,000 (and climbing) vulnerabilities being discovered each year, system and network administrators are in a difficult situation. They are challenged with keeping up with all the systems they have and all the patches released for those systems. Patches can be difficult to apply and might even have unexpected side effects. We have found that, after a vendor releases a security patch, it takes a long time for system administrators to fix all the vulnerable computer systems. It can be months or years before the patches are implemented on 90-95 percent of the vulnerable computers. For example, we still receive reports of outbreaks of the Melissa virus, which exploits vulnerabilities that are more than three years old.

There are a variety of reasons for the delay. The job might be too time-consuming, too complex, or just given too low a priority for the system administration staff to handle. With increased complexity comes the introduction of more vulnerabilities, so solutions do not solve problems for the long term—system maintenance is never-ending. Because many managers do not fully understand the risks, they neither give security a high enough priority nor assign adequate resources. Exacerbating the problem is the fact that the demand for skilled system administrators far exceeds the supply.

Even in an ideal situation, conscientious system administrators cannot adequately protect their computer systems because other system administrators and users, including home users, do not adequately protect *their* systems. Incident reports to the CERT/CC indicate that many people do not keep their anti-virus software up to date; and they do not apply patches to close vulnerabilities. Computers on the Internet are extremely interdependent. The security of each system on the Internet affects the security of every other system.

Reactive Solutions Have Limited Effectiveness

For the past 14 years, we have relied heavily on the ability of the Internet community as a whole to react quickly enough to security attacks to ensure that damage is minimized and attacks are quickly defeated. Today, however, it is clear that we are reaching the limits of effectiveness of our reactive solutions. While individual response organizations are all working hard to streamline and automate their procedures and are working together to better coordinate activities, a number of factors have combined to limit the effectiveness of reactive solutions:

- The number of vulnerabilities in commercial off-the-shelf software is now at the level that it is virtually impossible for any but the best resourced organizations to keep up with the vulnerability fixes.
- The Internet now connects over 162,000,000 computers and continues to grow at a rapid pace. At any point in time, there are hundreds of thousands of connected computers that are vulnerable to one form of attack or another.
- Attack technology has now advanced to the point where it is easy for attackers to take advantage of these vulnerable machines and harness them together to launch high-powered attacks.
- Many attacks are now fully automated and spread at nearly the speed of light across the entire Internet community.
- The attack technology has become increasingly complex and in some cases intentionally stealthy, thus increasing the time it takes to discover and analyze the attack mechanisms in order to produce antidotes.
- Internet users have become increasingly dependent on the Internet and now use it for many critical applications as well as online business transactions. Even relatively short interruptions in service cause significant economic loss and can jeopardize critical services.

These factors, taken together, indicate that we can expect many attacks to cause significant economic losses and service disruptions within even the best response times that we can realistically hope to achieve. Aggressive, coordinated response will continue to be necessary, but we must also move quickly to put other solutions in place.

Recommended Actions

Working our way out of the vulnerable position we are in requires a multi-pronged approach that helps us deal with the escalating near-term problem while at the same time building stronger foundations for the future. The work that must be done includes achieving these changes:

- Higher quality information technology products with security mechanisms that are better matched to the knowledge, skills, and abilities of today's system managers, administrators, and users
- Wider adoption of risk analysis and risk management policies and practices that help organizations identify their critical security needs, assess their operations and systems against those needs, and implement security improvements identified through the assessment process
- Expanded research programs that lead to fundamental advances in computer security
- A larger number of technical specialists who have the skills needed to secure large, complex systems
- Increased and ongoing awareness and understanding of cyber-security issues, vulnerabilities, and threats by all stakeholders in cyber space

Higher quality products: In today's Internet environment, a security approach based on "user beware" is unacceptable. The systems are too complex and the attacks happen too fast for this approach to work. Fortunately, good software engineering practices can dramatically improve our ability to withstand attacks. The solutions required are a combination of the following:

- Virus-resistant/virus-proof software – There is nothing intrinsic about digital computers or software that makes them vulnerable to viruses, which propagate and infect systems because of design choices that have been made by computer and software designers. Designs are susceptible to viruses and their effects when they allow the import of executable code, in one form or another, and allow the unconstrained execution of that code on the machine that received it. Unconstrained execution allows code developers to easily take full advantage of a system's capabilities, but does so with the side effect of making the system vulnerable to virus attack. To effectively control viruses in the long term, vendors must provide systems and software that constrain the execution of imported code, especially code that comes from unknown or untrusted sources. Some techniques to do this have been known for decades. Others, such as "sandbox" techniques, are more recent.
- Reducing implementation errors by at least two orders of magnitude – Most vulnerabilities in products come from software implementation errors. They remain in products, waiting to be discovered, and are fixed only after they are found while in use. Worse, the same flaws continue to be introduced in new products. Vendors need to be proactive, and adopt known, effective software engineering practices that dramatically reduce the number of flaws in software products.
- High-security default configurations – With the complexity of today's products, properly configuring systems and networks to use the strongest security built into the products is difficult, even for people with strong technical skills and training. Small mistakes can leave systems vulnerable and put users at risk. Vendors can help reduce the impact of security problems by shipping products with "out of the box" configurations that have security options turned on rather than require users to turn them on. The users can change these "default" configurations if desired, but they would have the benefit of starting from a secure base.

To encourage product vendors to produce the needed higher quality products, we encourage the government to use its buying power to demand higher quality software. The government should consider upgrading its contracting processes to include "code integrity" clauses, clauses that hold vendors more accountable for defects in released products. Included here as well are upgraded acquisition processes that place more emphasis on the security characteristics of systems being acquired. In addition, to support these new processes, training programs for acquisition professionals should be developed that provide training not only in current government security regulations and policies, but also in the fundamentals of security concepts and architectures. This type of skill building is needed in order to ensure that the government is acquiring systems that meet the spirit, as well as the letter, of the regulations.

Wider adoption of security practices: With our growing dependence on information networks and with the rapid changes in network technology and threats, it is critical that more organizations, large and small, adopt the use of effective information security risk assessments, management policies, and practices. While there is often discussion and debate over which particular body of practices might be in some way "best," it is clear that descriptions of effective practices and policy templates are widely available from both government and private sources. The Internet Security Alliance, for example, has recently published a "Common Sense Guide For Senior Mangers" that outlines the security management and technical practices an organization should adopt to improve its security. Guidelines and publications are also available from the National Institute of Standards and Technology, the National Security Agency, and other agencies. What is sometimes missing today is management commitment: senior management's visible endorsement of security improvement efforts and the provision of the resources needed to implement the required improvements.

Expanded research in information assurance: It is critical to maintain a long-term view and invest in research toward systems and operational techniques that yield networks capable of surviving attacks while protecting sensitive data. In doing so, it is essential to seek fundamental technological solutions and to seek proactive, preventive approaches, not just reactive, curative approaches.

Thus, the research agenda should seek new approaches to system security. These approaches should include design and implementation strategies, recovery tactics, strategies to resist attacks, survivability trade-off analysis, and the development of security architectures. Among the activities should be the creation of

- A unified and integrated framework for all information assurance analysis and design
- Rigorous methods to assess and manage the risks imposed by threats to information assets
- Quantitative techniques to determine the cost/benefit of risk mitigation strategies
- Systematic methods and simulation tools to analyze cascade effects of attacks, accidents, and failures across interdependent systems
- New technologies for resisting attacks and for recognizing and recovering from attacks, accidents, and failures

In this research program, special emphasis should be placed on the overlap between the cyber world and the physical world, and the analysis techniques developed should help policy and decision makers understand the physical impact and disruption of cyber attacks alone or of cyber attacks launched to amplify the impact of concurrent physical attacks.

More technical specialists: Government identification and support of cyber-security centers of excellence and the provision of scholarships that support students working on degrees in these universities are steps in the right direction. The current levels of support, however, are far short of what is required to produce the technical specialists we need to secure our systems and networks. These programs should be expanded over the next five years to build the university infrastructure we will need for the long-term development of trained security professionals.

More awareness and training for Internet users: The combination of easy access and user-friendly interfaces have drawn users of all ages and from all walks of life to the Internet. As a result, many Internet users have little understanding of Internet technology or the security practices they should adopt. To encourage "safe computing," there are steps we believe the government could take:

- Support the development of educational material and programs about cyberspace for all users. There is a critical need for education and increased awareness of the security characteristics, threats, opportunities, and appropriate behavior in cyberspace. Because the survivability of systems is dependent on the security of systems at other sites, fixing one's own systems is not sufficient to ensure those systems will survive attacks. Home users and business users alike need to be educated on how to operate their computers most securely, and consumers need to be educated on how to select the products they buy. Market pressure, in turn, will encourage vendors to release products that are less vulnerable to compromise.
- Support programs that provide early training in security practices and appropriate use. This training should be integrated into general education about computing. Children should learn early about acceptable and unacceptable behavior when they begin using computers just as they are taught about acceptable and unacceptable behavior when they begin using libraries.[2] Although this recommendation is aimed at elementary and secondary school teachers, they themselves need to be educated by security experts and professional organizations. Parents need be educated as well and should reinforce lessons in security and behavior on computer networks.

Conclusion

Interconnections across and among cyber and physical systems are increasing. Our dependence on these interconnected systems is also rapidly increasing, and even short-term disruptions can have major consequences. Cyber attacks are cheap, easy to launch, difficult to trace, and hard to prosecute. Cyber attackers are using the connectivity to exploit widespread vulnerabilities in systems to conduct criminal activities, compromise information, and launch denial-of-service attacks that seriously disrupt legitimate operations. Most threatening is the clear evidence that terrorists are investigating the feasibility of launching cyber attacks that could lead to devastating physical consequences.

Reported attacks against Internet systems are almost doubling each year and attack technology will evolve to support attacks that are even more virulent and damaging. Our current solutions are not keeping pace with the increased strength and speed of attacks, and our information infrastructures are at risk. Solutions are not simple, but must be pursued aggressively to allow us to keep our information infrastructures operating at acceptable levels of risk. However, we can make significant progress by making changes in software design and development practices, increasing the number of trained system managers and administrators, improving the knowledge

[2] National Research Council, *Computers at Risk: Safe Computing in the Information Age*, National Academy Press, 1991, recommendation 3c, p. 37.

level of users, and increasing research into secure and survivable systems. Additional government support for research, development, and education in computer and network security would have a positive effect on the overall security of the Internet.

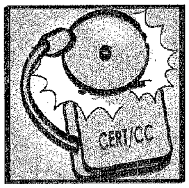
Survivable Systems Initiative
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

The Software Engineering Institute (SEI) is a federally funded research and development center at Carnegie Mellon University. The SEI has a unique mission—to be the steward for the discipline of software engineering. The SEI works with government and industry organizations, including the commercial sector, to help improve their software engineering capabilities.

While the SEI technical program is comprehensive, one unique area of work is focused on cyber defense. It is called the Survivable Systems Initiative to underscore the pervasive nature of the Internet and other networks in information systems. It is now necessary to design our systems to survive the consequences of faulty software. Most cyber attacks exploit defects in commercial software that are avoidable through the use of known engineering methods.

The Survivable Systems Initiative is recognized by government and industry alike as an authoritative, unbiased source of information assurance data and expertise. Here is a brief description of some key activities.

CERT® Coordination Center



The CERT/CC was established in 1988 as the first computer security incident response team (CSIRT). Staff members provide technical assistance and coordinate responses to security compromises, identify trends in intruder activity, analyze vulnerabilities in network products and systems, and work with vendors and other security experts to identify solutions to security problems. They alert the Internet community to potential threats to the security of their systems and provide information about how to avoid, minimize, or recover from the damage. In addition, the CERT/CC Knowledgebase contains information on vulnerabilities and threats and provides a facility for secure discussions.

The CERT/CC technical experts are routinely called upon by their sponsors and by international and homeland security leaders to identify and recommend remedies to security problems in the Internet infrastructure and to coordinate activity to implement those remedies.

Incident and Vulnerability Handling

The CERT/CC has responded to nearly 200,000 security incidents that have affected hundreds of thousands of Internet sites, has handled more than 8,000 reported vulnerabilities, has issued hundreds of advisories and bulletins, and has catalogued and disseminated information on thousands of vulnerabilities. In response to the exponential growth of incidents, the CERT/CC is developing an automated incident reporting system, AirCERT, whose sensors detect and report known methods of attacks.

Malicious Code Analysis

Because attacks on computer systems have become increasingly automated and sophisticated, the CERT/CC has added malicious code analysis to its activities; that is, they analyze the programs that intruders use for exploiting flaws in networked systems. For example, CERT/CC analysts reverse engineered the Nimda and Bad Trans worms and produced information on countermeasures.

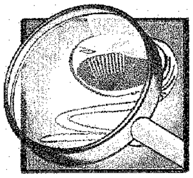
Building Computer Security Incident Response Teams
The CERT/CC has helped foster the creation of more than 200 computer security incident response teams. The scale of emerging networks and the diversity of user communities make it impractical for a single organization to provide universal support for addressing computer security issues. Therefore, the CERT/CC staff regularly works with sites to help them form CSIRTs.

CERT/CC staff members provide training courses for CSIRT managers and technical staff, give technical assistance by reviewing policies and standard operating procedures, and publish materials such as a CSIRT handbook, templates, and checklists. In addition, the staff is working on standards for certification and accreditation of Computer Network Defense Service Providers and CSIRTs.

The CERT/CC is funded by federal agencies including the U.S. Department of Defense, the Defense Information Systems Agency, the General Services Administration, the FBI, and the U.S. Secret Service, as well as other government and private organizations. The CERT/CC reaches the commercial sector through the Internet Security Alliance, a collaborative effort between the SEI, the CERT/CC, and the Electronic Industries Alliance (EIA).

CERT Analysis Center

The CERT Analysis Center has been established to assess and predict Internet threats, both current and potential threats. Analysts use a multi-disciplinary approach to analyze the threat environment from a number of perspectives, including political, economic, social, and technical motivations and impacts. The Internet is an expanding element of modern day society, and the effects of malicious activity have greater implications than ever before.

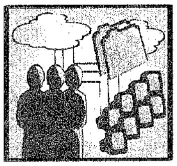


Their work includes developing techniques to do baseline mapping of large-scale datasets and to identify unauthorized and potentially malicious activity within overall network/system usage. They have been successful in isolating significant data that typically cannot be distinguished from the "noise" of system usage.

The CERT/AC staff has provided guidelines to help the U.S. Secret Service incorporate the cyber element into both investigations and preparations for protective activities such as national special security events. Other funders include the National Security Agency, the Department of State, and industry.

Survivable Enterprise Management

The Survivable Enterprise Management aspect of the Survivable Systems Initiative takes a strategic, enterprise-wide approach to managing information security risk. The staff defines and transitions organizational and technical security practices and methodologies to help organizations evaluate, improve, and maintain the security of their systems. Two of these are OCTAVE^{SM} and CERT security practices.

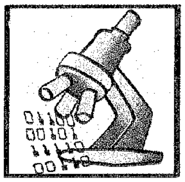


The **Operationally Critical Threat Asset and Vulnerability Evaluation (OCTAVE^{SM})** defines a self-directed approach to identifying and managing information security risks.

OCTAVE enables an enterprise to identify the information assets that are important to its mission, the threats to those assets, and vulnerabilities that could expose the information to the threats. The outcome is an protection strategy to reduce risk. Staff members have published a comprehensive reference guide for organizations' internal analysis teams: the *OCTAVE Method Implementation Guide.* In addition, the OCTAVE approach is described in a book published by Addison-Wesley entitled *Managing Information Security Risks: The OCTAVE Approach.*

CERT security practices are practical steps experienced system administrators can take to protect networked computer systems from malicious and inadvertent security compromises. The practices are technology-neutral for broad application. The current set of fifty practices is defined in *The CERT Guide to System and Network Security Practices* book and in security improvement modules on the CERT web site.

Research: Survivable Network Technology



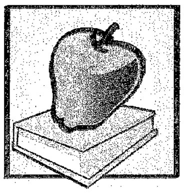
As the Internet and networked systems become more and more widespread and advanced, there is a higher risk of accidents, attacks, and failures. Survivable Systems researchers are working on technological approaches to preventing security flaws. They research ways to ensure that the computers still provide the most important services even if there is a security compromise.

One aspect of the research is in the field of **survivable systems engineering**, which explores the current state of systems to identify problems and propose engineering solutions. The overall objective is to improve system engineering practices for survivability. The work includes analysis of how susceptible these systems are to sophisticated attacks and finding ways to improve the design of systems.

The research agenda has its roots in the **Survivable Systems Analysis** (SSA), which is already in use. SSA is a process for analyzing survivability at the architecture level. It identifies "soft spots" in proposed new architectures, allowing designers and developers to "harden" the product or network before it is built. SSA can also be used on operational systems, helping sites prioritize improvements.

Other researchers concentrate on **modeling and simulation.** For example, the Easel system is being used to study network responses to attacks and attack mitigation strategies. In essence, Easel is a survivability tool for managing computer security risks. One demonstration predicts the effectiveness of software patching during a widespread computer virus event—it is possible to investigate what critical factors determine the outcome. Easel is currently distributed widely as a beta-test release to the Department of Defense and Internet community.

Education and Training



Networked systems allow organizations to access information rapidly, improve communications, collaborate with partners, provide better customer service, and conduct electronic business. The challenge is to educate individuals within enterprises to improve the security and survivability of globally interconnected infrastructures. The Survivable Systems Initiative offers public training courses for technical staff and managers of computer security incident response teams as well as for system administrators and other technical personnel interested in learning more about network security.

Staff members also conduct training needs analysis in the area of information security, and they define and develop curricula. In addition, the staff is collaborating with the Carnegie Mellon University H. J. Heinz III School of Public Policy and Management to develop a curriculum in information security management, and several staff members teach courses in the program.

Survivable Systems staff, along with Carnegie Mellon faculty members, are working with historically black colleges and universities and Hispanic-serving institutions on a program designed to create a next generation of Internet-security experts. The program will provide the participants with the knowledge and expertise to develop and deliver curricula in information security. It will increase the number of Ph.D.-level researchers in information security at these colleges and universities.

The Survivable Systems Initiative education and training activities help fill the gap between the number of security experts needed and the number available.

Supporting National Efforts

Survivable Systems Initiative staff members have long been involved in national efforts relating to network security, providing advice and assistance to government leaders and testifying before Congressional committees. Specific groups that have requested assistance and information include the National Threat Assessment Center, the National Security Council, the National Infrastructure Protection Center, the President's Critical Infrastructure Protection Board, the board's Cyber Interagency Working Group, and the Office of Management and Budget/General Services Administration Electronic Government Initiatives.

The CERT/CC staff has also been active in Internet standards bodies such as the Internet Engineering Task Force.

Mr. HORN. Thank you. I'd like to still know what CERT is. And I've looked through here. You've got all sorts of things that you could put in there. But, you know, is it the Center on Readiness and Training and so forth?

Mr. PETHIA. Computer Emergency Response Team.

Mr. HORN. OK. Good enough. You've got a busy type, and we thank you for all the things you've done for us and the various people in this town. So thank you for having that very fine university in that very fine CERT Coordination Center.

Mr. HORN. We now go to the last presenter, Robert F. Dacey, Director, Information Security, U.S. General Accounting Office, and headed by the Controller General of the United States. And you and your staff have done a marvelous position every year, helping us look at this material when they come in to the Office of Management and Budget. So, Director Dacey.

Mr. DACEY. Mr. Chairman and Mr. Lewis, it is a pleasure to be here this morning. And before providing my testimony, however, I would like to thank you personally, Mr. Chairman for your sustained and dedicated efforts to improving Federal information technology management especially in the areas of Y2K and information security, and, from my prior experience, your extreme interest in improving financial management throughout the Federal Government. Your tireless vigilance has resulted in increased attention to these important areas and has stimulated many positive results.

As you requested, I will briefly summarize my written statement. Federal agencies rely extensively on computerized systems and electronic data to support their missions. If these systems are inadequately protected, resources such as Federal payments and collections could be lost or stolen. Computer resources could be used for unauthorized purposes or to launch attacks on others. Sensitive information such as taxpayer data and proprietary business information could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime. Critical operations such as those supporting national defense and emergency services could be disrupted. Data could be modified or destroyed for purposes of fraud, deception, or disruption. And agency missions could be undermined by embarrassing incidents that result in diminished confidence in their ability to conduct operations and to fulfill their fiduciary responsibilities.

As Mr. Pethia pointed out, the risks are dramatically increasing over the years and have been. There are a lot of reasons for this which he discussed and I would like to again highlight. First of all, with its greater complexity and interconnectivity of systems, including within Federal systems and between Federal systems and other systems in many cases, trusted relationships exist between these systems which allow open access if someone breaks into one of the systems.

Second, standardization of systems hardware and software, which combined with known vulnerabilities create significant exposures.

Third, the increased volume, sophistication, and effectiveness of cyber attacks, which combines with the readily available intrusion or hacking tools and limited capabilities to detect such attacks.

And, fourth, the development of cyber attack capabilities by other nations, terrorists, criminals, and intelligence services. In addition to the threat of external attacks, the disgruntled insider is also a significant threat because such individuals often have knowledge that allows them to gain restricted access and inflict damage or steal assets.

While both the threat and ease of cyber attack are increasing, our most recent analysis of reports issued since October 2001 continues to show significant, pervasive weaknesses in Federal unclassified computer systems that put critical Federal operations and assets at risk. We have reported on the potentially devastating consequences of poor information security since September 1996 and have identified information security as a high risk area since 1997.

Our chart, which is on the right here, illustrates the significant weaknesses that were reported for each of the 24 agencies included in our review, which covers the six major areas of general controls; that is, those areas that cover either all or a major portion of an agency's information systems and help to ensure their proper operation.

As the chart shows, most agencies had significant weaknesses in many or all of the control areas, and efforts to expand and improve information security may result in additional significant deficiencies being identified. Also, all agencies had weaknesses in security program management which can often lead to weaknesses in other control categories.

At the same time, a number of actions to improve information security are underway, both at an agency- and governmentwide level. Some of these actions may require time to fully implement and address all of the significant weaknesses that have been identified.

Implementation of Government Information Security Reform, commonly known as GISRA, is proving to be a significant step in improving Federal agency information security. We are pleased to note that Congress has recently passed legislation to continue and improve these efforts. In its fiscal 2001 report to Congress on GISRA, OMB acknowledged the information security challenges faced by the Federal Government and highlighted six common security weaknesses, which Mr. Forman earlier discussed. Highlighting weaknesses through GISRA reviews, evaluations, and reporting helps agencies to undertake corrective actions. Also many agencies reported that first-year implementation has resulted in increased management attention and created a baseline for future reviews.

In addition, GISRA implementation has resulted in important actions by the administration, which, if properly implemented, should continue to improve information security in the Federal Government. Mr. Forman previously highlighted these actions in his testimony and some of the new actions they are taking. In addition, the President has taken broader actions in the areas of homeland security and critical infrastructure protection that also can lead to improvements in Federal information security.

In addition to these actions, GAO believes that there are a number of important steps the administration and agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include: Delineating the roles and responsibilities of the numerous entities involved in Federal information security and CIP or Critical Infrastructure Protection; providing more specific guidance on controls agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls allocating sufficient resources for information security; and continuing research and development efforts to find new ways to manage information security better.

Mr. Chairman, Mr. Lewis, this concludes my statement. I'll be pleased to answer any questions that you have at this time.

[The prepared statement of Mr. Dacey follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m. EST
Tuesday,
November 19, 2002

COMPUTER SECURITY

Progress Made, But Critical Federal Operations And Assets Remain at Risk

Statement of Robert F. Dacey
Director, Information Security Issues

GAO
Accountability * Integrity * Reliability

GAO
Accountability·Integrity·Reliability

Highlights

Highlights of GAO-03-303T, a testimony before the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives.

November 2002

COMPUTER SECURITY

Progress Made, But Critical Federal Operations and Assets Remain at Risk

Why GAO Did This Study

Protecting the computer systems that support our critical operations and infrastructures has never been more important because of the concern about attacks from individuals and groups with malicious intent, including terrorism. These concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information. At the subcommittee's request, GAO discussed its analysis of recent information security audits and evaluations at 24 major federal departments and agencies.

www.gao.gov/cgi-bin/getrpt?GAO-03-303T.

To view the full testimony, click on the link above. For more information, contact Robert F. Dacey at (202) 512-3317 or daceyr@gao.gov.

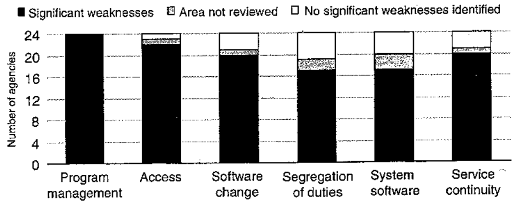
What GAO Found

Although GAO's current analyses of audit and evaluation reports for the 24 major departments and agencies issued from October 2001 to October 2002 indicate some individual agency improvements, overall they continue to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. GAO identified significant weaknesses in each of the 24 agencies in each of the six major areas of general controls. As in 2000 and 2001, weaknesses were most often identified in control areas for security program management and access controls. All 24 agencies had weaknesses in security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented (see figure below for list of major weaknesses).

Implementation of the Government Information Security Reform provisions ("GISRA") is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as integrating security into the President's Management Agenda Scorecard. However, GISRA is scheduled to expire on November 29, 2002. GAO believes that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses.

In addition to reauthorizing this legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Information Security Weaknesses at 24 Major Agencies



Source: Audit reports issued October 2001 through October 2002.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss our analyses of recent information security audits and evaluations at federal agencies. As with other large organizations, federal agencies rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, as well as to helping prevent data tampering, fraud, and inappropriate disclosure of sensitive information.

Our analyses considered the results of information security audits and evaluations reported by GAO and inspectors general (IGs) from October 2001 to October 2002 for 24 major federal departments and agencies. In summarizing these results, I will (1) discuss the continuing pervasive weaknesses that led GAO to initially begin reporting information security as a governmentwide high-risk issue in 1997, (2) illustrate the serious risks that these weaknesses pose at selected individual agencies, and (3) describe the major common weaknesses that agencies need to address to improve their information security programs, including agencies' weaknesses in meeting the security requirements of Government Information Security Reform legislation (commonly referred to as "GISRA").[1] Finally, I will discuss some positive actions taken or planned by the administration to improve federal information security, as well as the additional steps needed to develop a comprehensive governmentwide strategy for improvement.

We performed our analyses from September 2002 to November 2002 in accordance with generally accepted government auditing standards.

Results in Brief

Protecting the computer systems that support our nation's critical operations and infrastructures has never been more important. Telecommunications, power distribution, water supply, public health services, national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. Yet with this dependency comes an increasing concern about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence

[1] Title X, Subtitle G—Government Information Security Reform, Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001, P.L. 106-398, October 30, 2000.

gathering, and acts of war. Such concerns are well founded for a number of reasons, including the dramatic increases in reported computer security incidents, the ease of obtaining and using hacking tools, the steady advance in the sophistication and effectiveness of attack technology, and the dire warnings of new and more destructive attacks.

Although our current analyses of audit and evaluation reports for the 24 major departments and agencies indicate some individual agency improvements, overall they continue to highlight significant information security weaknesses that place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, resources, such as federal payments and collections, could be lost or stolen; sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed or browsed or copied for purposes of espionage or other types of crime; and critical operations, such as those supporting national defense and emergency services, could be disrupted.

We identified significant weaknesses in each of the 24 agencies covered by our review and in each of the following six major areas of general controls, that is, the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These areas are *security program management*, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; *access controls*, which ensure that only authorized individuals can read, alter, or delete data; *software development and change controls*, which ensure that only authorized software programs are implemented; *segregation of duties*, which reduces the risk that one individual can independently perform inappropriate actions without detection; *system software controls*, which protect sensitive programs that support multiple applications from tampering and misuse; and *service continuity*, which ensures that computer-dependent operations experience no significant disruptions. As in past years' analyses, we identified weaknesses most often for security program management and access controls.

Implementation of GISRA is proving to be a significant step in improving federal agencies' information security programs. It has also prompted the administration to take important actions to address information security, such as plans to integrate security into the President's Management Agenda Scorecard. Although legislation that would reauthorize GISRA is currently being considered, GISRA is scheduled to expire in less than 2 weeks. We believe that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses.

In addition to Congress' reauthorizing information security legislation, there are a number of important steps that the administration and the agencies should take to ensure that information security receives appropriate attention and resources and that known deficiencies are addressed. These steps include delineating the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection; providing more specific guidance on the controls that agencies need to implement; obtaining adequate technical expertise to select, implement, and maintain controls to protect information systems; and allocating sufficient agency resources for information security.

Background

Dramatic increases in computer interconnectivity, especially in the use of the Internet, continue to revolutionize the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often 24 hours a day; and electronic mail, Internet Web sites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of individuals and groups.

In addition to such benefits, however, this widespread interconnectivity poses significant risks to the government's and our nation's computer systems and, more important, to the critical operations and infrastructures they support. For example, telecommunications, power distribution, water supply, public health services, and national defense (including the military's warfighting capability), law enforcement, government services, and emergency services all depend on the security of their computer operations. The speed and accessibility that create the enormous benefits of the computer age likewise, if not properly controlled, allow individuals and organizations to inexpensively eavesdrop on or interfere with these operations from remote locations for mischievous or malicious purposes, including fraud or sabotage.

Government officials are increasingly concerned about attacks from individuals and groups with malicious intent, such as crime, terrorism, foreign intelligence gathering, and acts of war. According to the Federal

Bureau of Investigation (FBI), terrorists, transnational criminals, and intelligence services are quickly becoming aware of and using information exploitation tools such as computer viruses, Trojan horses, worms, logic bombs, and eavesdropping sniffers that can destroy, intercept, degrade the integrity of, or deny access to data.[2] In addition, the disgruntled organization insider is a significant threat, since such individuals often have knowledge that allows them to gain unrestricted access and inflict damage or steal assets without possessing a great deal of knowledge about computer intrusions. As greater amounts of money are transferred through computer systems, as more sensitive economic and commercial information is exchanged electronically, and as the nation's defense and intelligence communities increasingly rely on commercially available information technology, the likelihood increases that information attacks will threaten vital national interests.

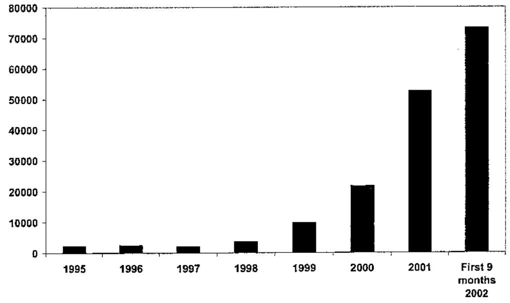
As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A potential hacker can literally download tools from the Internet and "point and click" to start a hack. Experts also agree that there has been a steady advance in the sophistication and effectiveness of attack technology. Intruders quickly develop attacks to exploit vulnerabilities discovered in products, use these attacks to compromise computers, and share them with other attackers. In addition, they can combine these attacks with other forms of technology to develop programs that automatically scan the network for vulnerable systems, attack them, compromise them, and use them to spread the attack even further.

The April 2002 annual report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the FBI's San Francisco Computer Intrusion Squad, showed that 90 percent of respondents (primarily large corporations and government agencies) had

[2] *Worm*: an independent computer program that reproduces by copying itself from one system to another across a network. Unlike computer viruses, worms do not require human involvement to propagate. *Virus*: a program that "infects" computer files, usually executable programs, by inserting a copy of itself into the file. These copies are usually executed when the "infected" file is loaded into memory, allowing the virus to infect other files. Unlike the computer worm, a virus requires human involvement (usually unwitting) to propagate. *Trojan horse*: a computer program that conceals harmful code. A Trojan horse usually masquerades as a useful program that a user would wish to execute. *Logic bomb*: in programming, a form of sabotage in which a programmer inserts code that causes the program to perform a destructive action when some triggering event occurs, such as terminating the programmer's employment. *Sniffer*: synonymous with packet sniffer. A program that intercepts routed data and examines each packet in search of specified information, such as passwords transmitted in clear text.

detected computer security breaches. In addition, the number of computer security incidents reported to the CERT® Coordination Center rose from 9,859 in 1999 to 52,658 in 2001 and 73,359 for just the first 9 months of 2002.[3] And these are only the reported attacks. The Director, CERT® Centers, stated that he estimates that as much as 80 percent of actual security incidents goes unreported, in most cases because (1) the organization was unable to recognize that its systems had been penetrated or there were no indications of penetration or attack, or (2) the organization was reluctant to report. Figure 1 shows the number of incidents reported to the CERT® Coordination Center from 1995 through the first 9 months of 2002.

Figure 1: Information Security Incidents Reported to Carnegie-Mellon's CERT® Coordination Center from 1995 to the First 9 Months of 2002



Source: Carnegie-Mellon's CERT® Coordination Center.

The risks posed by this increasing and evolving threat are demonstrated in reports of actual attacks and disruptions, as well as by continuing government warnings. For example:

[3] CERT® Coordination Center (CERT-CC) is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University.

- Just last week, news reports indicated that a British computer administrator was indicted on charges that he broke into 92 U.S. computer networks in 14 states belonging to the Pentagon, private companies, and the National Aeronautics and Space Administration during the past year, causing some $900,000 in damage to computers. It also reported that, according to a Justice Department official, these attacks were one of the biggest hacks ever against the U.S. military. This official also said that the attacker used his home computer and automated software available on the Internet to scan tens of thousands of computers on U.S. military networks looking for ones that might suffer from flaws in Microsoft Corporation's Windows NT operating system software.

- The FBI's National Infrastructure Protection Center (NIPC) reported that on October 21, 2002, all of the 13 root-name servers that provide the primary roadmap for almost all Internet communications were targeted in a massive "distributed denial of service" attack. Seven of the servers failed to respond to legitimate network traffic, and two others failed intermittently during the attack. Because of safeguards, most Internet users experienced no slowdowns or outages. However, according to the media reports, a longer, more extensive attack could have seriously damaged worldwide electronic communications.

- In September 2002, NIPC issued a warning of cyber attacks against the International Monetary Fund and World Bank meetings to be held during the week of September 23.[4] The warning stated that, in addition to physical protestors, cyber groups might view the meetings as a platform to display their hacking talent or to propagate a specific message. Cyber protestors, referred to as "hacktivists," can engage in Web page defacements, denial-of-service attacks, and misinformation campaigns, among other attacks.

- In July 2002, NIPC reported that the potential for compound cyber and physical attacks, referred to as "swarming attacks," is an emerging threat to the U.S. critical infrastructure.[5] As NIPC reports, the effects of a swarming attack include slowing or complicating the response to a physical attack. For example, cyber attacks can be used to delay the notification of emergency services and to deny the resources needed to manage the consequences of a physical attack. In addition, a swarming attack could be used to worsen the effects of a physical attack. For

[4] National Infrastructure Protection Center, Assessment 02-002: *Hacktivism in Connection with Protest Events of September 2002* (Washington, D.C.: Sept. 23, 2002)

[5] National Infrastructure Protection Center, *Swarming Attacks: Infrastructure Attacks for Destruction and Disruption* (Washington, D.C.: July 2002).

instance, a cyber attack on a natural gas distribution pipeline that opens safety valves and releases fuels or gas in the area of a planned physical attack could enhance the force of the physical attack. Consistent with this threat, NIPC also released an information bulletin in April 2002 warning against possible physical attacks on U.S. financial institutions by unspecified terrorists.[6]

- In August 2001, we reported to this subcommittee that the attacks referred to as Code Red, Code Red II, and SirCam had affected millions of computer users, shut down Web sites, slowed Internet service, and disrupted business and government operations.[7] Then in September 2001, the Nimda worm appeared using some of the most significant attack profile aspects of Code Red II and 1999's infamous Melissa virus that allowed it to spread widely in a short amount of time. Security experts estimate that Code Red, Sircam, and Nimda have caused billions of dollars in damage.

Since the September 11, 2001, attacks, warnings of the potential for terrorist cyber attacks against our critical infrastructures have also increased. For example, in February 2002, the Special Advisor to the President for Cyberspace Security stated in a Senate briefing that although to date none of the traditional terrorist groups such as al Qaeda have used the Internet to launch a known attack on the United States infrastructure, information on computerized water systems was discovered on computers found in al Qaeda camps in Afghanistan. Also, in his February 2002 statement for the Senate Select Committee on Intelligence, the director of central intelligence discussed the possibility of cyber warfare attack by terrorists.[8] He stated that the September 11 attacks demonstrated the nation's dependence on critical infrastructure systems that rely on electronic and computer networks. Further, he noted that attacks of this nature will become an increasingly viable option for terrorists as they and other foreign adversaries become more familiar with these targets and the technologies required to attack them.

[6] National Infrastructure Protection Center, *Possible Terrorism Targeting of US Financial System–Information Bulletin 02-003* (Washington, D.C.: Apr. 19, 2002).

[7] U.S. General Accounting Office, *Information Security: Code Red, Code Red II, and SirCam Attacks Highlight Need for Proactive Measures;* GAO-01-1073T (Washington, D.C.: Aug. 29, 2001).

[8] Testimony of George J. Tenet, Director of Central Intelligence, before the Senate Select Committee on Intelligence, Feb. 6, 2002.

Concerned with accounts of attacks on commercial systems via the Internet and reports of significant weaknesses in federal computer systems that make them vulnerable to attack, on October 30, 2000, Congress enacted GISRA, which became effective November 29, 2000, and is in effect for 2 years. GISRA supplements information security requirements established in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995, and the Clinger-Cohen Act of 1996 and is consistent with existing information security guidance issued by the Office of Management and Budget (OMB)[9] and the National Institute of Standards and Technology (NIST),[10] as well as audit and best practice guidance issued by GAO.[11] Most importantly, however, GISRA consolidates these separate requirements and guidance into an overall framework for managing information security and establishes new annual review, independent evaluation, and reporting requirements to help ensure agency implementation and both OMB and congressional oversight.

GISRA assigned specific responsibilities to OMB, agency heads and chief information officers (CIOs), and the IGs. OMB is responsible for establishing and overseeing policies, standards and guidelines for information security. This includes the authority to approve agency information security programs, but delegates OMB's responsibilities regarding national security systems to national security agencies. OMB is also required to submit an annual report to the Congress summarizing results of agencies' evaluations of their information security programs. GISRA does not specify a date for this report, and OMB released its fiscal year 2001 report in February 2002.

GISRA requires each agency, including national security agencies, to establish an agencywide risk-based information security program to be overseen by the agency CIO and ensure that information security is practiced throughout the life cycle of each agency system. Specifically, this program is to include

[9] Primarily OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," February 1996.

[10] Numerous publications made available at http://www.itl.nist.gov/ including National Institute of Standards and Technology, *Generally Accepted Principles and Practices for Securing Information Technology Systems,* NIST Special Publication 800-14, September 1996.

[11] U.S. General Accounting Office, *Federal Information System Controls Manual, Volume 1—Financial Statement Audits,* GAO/AIMD-12.19.6 (Washington, D.C.: January 1999); *Information Security Management: Learning from Leading Organizations,* GAO/AIMD-98-68 (Washington, D.C.: May 1998).

- periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems, and to data supporting critical operations and assets;
- the development and implementation of risk-based, cost-effective policies and procedures to provide security protections for information collected or maintained by or for the agency;
- training on security responsibilities for information security personnel and on security awareness for agency personnel;
- periodic management testing and evaluation of the effectiveness of policies, procedures, controls, and techniques;
- a process for identifying and remediating any significant deficiencies;
- procedures for detecting, reporting and responding to security incidents; and
- an annual program review by agency program officials.

In addition to the responsibilities listed above, GISRA requires each agency to have an annual independent evaluation of its information security program and practices, including control testing and compliance assessment. The evaluations of non-national-security systems are to be performed by the agency IG or an independent evaluator, and the results of these evaluations are to be reported to OMB. For the evaluation of national security systems, special provisions include designation of evaluators by national security agencies, restricted reporting of evaluation results, and an audit of the independent evaluation performed by the IG or an independent evaluator. For national security systems, only the results of each audit of an evaluation are to be reported to OMB.

Finally, GISRA also assigns additional responsibilities for information security policies, standards, guidance, training, and other functions to other agencies. These agencies are NIST, the Department of Defense, the Intelligence Community, the Attorney General, the General Services Administration, and the Office of Personnel Management.

Weaknesses in Federal Systems Remain Pervasive

Since September 1996, we have reported that poor information security is a widespread federal problem with potentially devastating consequences.[12] Although agencies have taken steps to redesign and strengthen their information system security programs, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from computer-based threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In addition, in 1998, 2000, and 2001, we analyzed audit results for 24 of the largest federal agencies and found that all 24 had significant information security weaknesses.[13] As a result of these analyses, we have identified information security as a governmentwide high-risk issue in reports to the Congress since 1997—most recently in January 2001.[14]

Our most recent analyses, of reports issued from October 2001 through October 2002, continue to show significant weaknesses in federal computer systems that put critical operations and assets at risk. Weaknesses continued to be reported in each of the 24 agencies included in our review, and they covered all six major areas of general controls—the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. These six areas are (1) security program management, which provides the framework for ensuring that risks are understood and that effective controls are selected and properly implemented; (2) access controls, which ensure that only authorized individuals can read, alter, or delete data; (3) software development and change controls, which ensure that only authorized software programs are implemented; (4) segregation of duties, which reduces the risk that one individual can independently perform inappropriate actions without detection; (5) operating systems

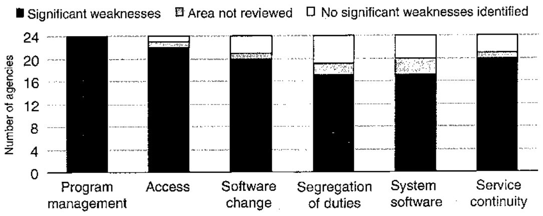
[12] U.S. General Accounting Office, *Information Security: Opportunities for Improved OMB Oversight of Agency Practices.* GAO/AIMD-96-110 (Washington, D.C.: Sept. 24, 1996).

[13] U.S. General Accounting Office, *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk,* GAO/AIMD-98-92 (Washington, D.C.: Sept. 23, 1998); *Information Security: Serious and Widespread Weaknesses Persist at Federal* Agencies, GAO/AIMD-00-295 (Washington, D.C.: Sept. 6, 2000); and *Computer Security: Improvements Needed to Reduce Risk to Critical Federal Operations and Assets,* GAO-02-231T (Washington, D.C.: Nov. 9, 2001).

[14] U.S. General Accounting Office, *High-Risk Series: Information Management and Technology,* GAO/HR-97-9 (Washington, D.C.: Feb. 1, 1997); *High-Risk Series: An Update,* GAO/HR-99-1 (Washington, D.C.: January 1999); *High Risk Series: An Update,* GAO-01-263 (Washington, D.C.: January 2001).

controls, which protect sensitive programs that support multiple applications from tampering and misuse; and (6) service continuity, which ensures that computer-dependent operations experience no significant disruptions. Figure 2 illustrates the distribution of weaknesses for the six general control areas across the 24 agencies.

Figure 2: Computer Security Weaknesses at 24 Major Federal Agencies



Source: Audit reports issued October 2001 through October 2002.

Although our current analyses showed that most agencies had significant weaknesses in these six control areas, as in past years' analyses, weaknesses were most often identified for security program management and access controls.

- For *security program management*, we identified weaknesses for all 24 agencies in 2002—the same as reported for 2001, and compared to 21 of the 24 agencies (88 percent) in 2000. Security program management, which is fundamental to the appropriate selection and effectiveness of the other categories of controls, covers a range of activities related to understanding information security risks; selecting and implementing controls commensurate with risk; and ensuring that controls, once implemented, continue to operate effectively.

- For *access controls*, we found weaknesses for 22 of 24 agencies (92 percent) in 2002 (no significant weaknesses were found for one agency, and access controls were not reviewed for another). This compares to access control weaknesses found in all 24 agencies for both 2001 and 2000. Weak access controls for sensitive data and systems make it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with only minimal computer and telecommunications resources and expertise.

In addition, it should also be emphasized that our current analyses showed service-continuity-related weaknesses at 20 of the 24 agencies (83 percent) with no significant weaknesses found for 3 agencies (service continuity controls were not reviewed for another). This compares to 19 agencies with service continuity weaknesses found in 2001 and 20 agencies found in 2000. Service continuity controls are important in that they help ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. If service continuity controls are inadequate, an agency can lose the capability to process, retrieve, and protect electronically maintained information, which can significantly affect an agency's ability to accomplish its mission. Further, such controls are particularly important in the wake of the terrorist attacks of September 11, 2001.

Our current analyses of information security at federal agencies also showed that the scope of audit work performed has continued to expand to more fully cover all six major areas of general controls at each agency. Not surprisingly, this has led to the identification of additional areas of weakness at some agencies. These increases in reported weaknesses do not necessarily mean that information security at federal agencies is getting worse. They more likely indicate that information security weaknesses are becoming more fully understood—an important step toward addressing the overall problem. Nevertheless, the results leave no doubt that serious, pervasive weaknesses persist. As auditors increase their proficiency and the body of audit evidence expands, it is probable that additional significant deficiencies will be identified.

Most of the audits represented in figure 2 were performed as part of financial statement audits. At some agencies with primarily financial missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at agencies whose missions are primarily nonfinancial, such as DOD and the Department of Justice, the audits may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluations of individual systems supporting nonfinancial operations. However, in response to congressional interest, beginning in fiscal year 1999, we expanded our audit focus to cover a wider range of nonfinancial operations—a trend we expect to continue. Audit coverage for nonfinancial systems has also increased as agencies and their IGs review and evaluate their information security programs as required by GISRA.

As previously reported, information security weaknesses are also indicated by limited agency progress in implementing Presidential Decision Directive (PDD) 63 to protect our nation's critical infrastructures from computer-based attacks. Issued in May 1998, PDD 63 established critical infrastructure protection as a national goal and called for a range of activities to improve federal agency security programs, establish a partnership between the government and the private sector, and improve the nation's ability to detect and respond to serious attacks. Critical infrastructure protection involves activities that enhance the security of our nation's cyber and physical public and private infrastructure that are essential to national security, national economic security, and/or national public health and safety. Federal agencies and other public and private entities rely extensively on computerized systems and electronic data to support their missions. Accordingly, the security of these systems and data is essential to avoiding disruptions in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information.

Last year, the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency (PCIE/ECIE) reported on the federal government's compliance with PDD 63. It concluded that the federal government could improve its planning and assessment activities for cyber-based critical infrastructures. Specifically, the council stated that (1) many agency infrastructure plans were incomplete; (2) most agencies had not identified their mission-critical infrastructure assets; and (3) few agencies had completed vulnerability assessments of mission-critical assets or developed remediation plans. Our subsequent review of PDD 63-related activities at eight lead agencies found similar problems.[15] For example, although most of the agencies we reviewed had identified critical assets, many had not completed related vulnerability assessments. Further, most of the agencies we reviewed had not taken the additional steps to identify interdependencies and, as a result, some agency officials said that they were not sure which of their assets were critical from a national perspective and, therefore, subject to PDD 63. Identifying interdependencies is important so that infrastructure owners can determine when disruption in one infrastructure could result in damage to other infrastructures.

[15] U.S. General Accounting Office, *Combating Terrorism: Selected Challenges and Related Recommendations*, GAO-01-822 (Washington, D.C.: September 20, 2001).

In addition, our review of fiscal year 2001 GISRA implementation showed that of the 24 large agencies we reviewed, 15 had not implemented an effective methodology, such as Project Matrix™ reviews, to identify their critical assets.[16] The Department of Commerce's Critical Infrastructure Assurance Office (CIAO) established Project Matrix™ to provide a standard methodology for identifying all assets, nodes, networks, and associated infrastructure dependencies and interdependencies required for the federal government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people. In addition, in an effort to more clearly identify and prioritize the security needs for government assets, in February 2002 OMB reported that it planned to direct all large agencies to undertake a Project Matrix™ review to identify critical infrastructure assets and their interdependencies with other agencies and the private sector. As of July 2002, CIAO reported that most agencies had not completed Project Matrix™ step 1 to identify their critical assets, and few had even begun step 2 to identify other federal government assets, systems, and networks on which their critical assets depend to operate.

Substantial Risks Persist for Federal Operations, Assets, and Confidentiality

To fully understand the significance of the weaknesses we identified, it is necessary to link them to the risks they present to federal operations and assets. 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. Hence, the degree of risk caused by security weaknesses is extremely high.

The weaknesses identified place a broad array of federal operations and assets at risk. For example,

- resources, such as federal payments and collections, could be lost or stolen;
- computer resources could be used for unauthorized purposes or to launch attacks on others;

[16] U.S. General Accounting Office, *Information Security: Additional Actions Needed to Implement Reform Legislation*, GAO-02-470T (Washington, D.C.: Mar. 6, 2002).

- sensitive information, such as taxpayer data, social security records, medical records, and proprietary business information, could be inappropriately disclosed, browsed, or copied for purposes of espionage or other types of crime;
- critical operations, such as those supporting national defense and emergency services, could be disrupted;
- data could be modified or destroyed for purposes of fraud or disruption; or
- agency missions could be undermined by embarrassing incidents that result in diminished confidence in the agencies' ability to conduct operations and fulfill their fiduciary responsibilities.

Recent audits show that while agencies have made some progress, weaknesses continue to be a problem and that critical federal operations and assets remain at risk.

- In February 2002, we reported that the Internal Revenue Service (IRS) corrected or mitigated many of the computer security weaknesses identified in our previous reports, but much remains to be done to resolve the significant control weaknesses that continue to exist within IRS's computing environment and to be able to promptly address new security threats and risks as they emerge.[17] Weaknesses found, such as not always adequately restricting electronic access within its computer networks and to its systems, can impair the agency's ability to perform vital functions and increase the risk that unauthorized individuals could gain access to critical hardware and software and intentionally or inadvertently view, alter, or delete sensitive data or computer programs. Also, such weaknesses increase the risk that individuals could obtain personal taxpayer information and use it to commit financial crimes in taxpayers' names (identity fraud), such as establishing credit and incurring debt.
- In April 2002, the IG for the Department of Justice reported serious deficiencies in controls for five sensitive-but-unclassified systems that support critical departmental functions, such as tracking prisoners; collecting, processing, and disseminating unclassified intelligence information; and providing secure information technology facilities,

[17] U.S. General Accounting Office, *Financial Audit: IRS's Fiscal Year 2001 and 2000 Financial Statements*, GAO-02-414 (Washington, D.C.: Feb. 27, 2002).

computing platforms, and support services.[18] The most significant of these deficiencies concerned the technical controls that help prevent unauthorized access to system resources. Because of the repetitive nature of the security deficiencies and concerns identified, the IG recommended that a central office responsible for system security be established to identify trends and enforce uniform standards. The IG also included other specific recommendations intended to improve departmentwide computer security for both classified and sensitive-but-unclassified systems. In addition to this report, in March 2002, the Commission for Review of FBI Security Programs reported that the FBI's information systems security controls were inadequate.

- In June 2002, we reported that the U.S. Army Corps of Engineers had made substantial progress in improving computer controls at each of its data processing centers and other Corps sites since our 1999 review, but that continuing and numerous newly identified control vulnerabilities continued to impair the Corps' ability to ensure the reliability, confidentiality, and availability of financial and sensitive data.[19] These vulnerabilities warranted management's attention to decrease the risk of inappropriate disclosure and modification of data and programs, misuse of or damage to computer resources, or disruption of critical operations. These vulnerabilities also increased risks to other DOD networks and systems to which the Corps' network is linked.

- In our September 2002 testimony, we reported that the Department of Veterans Affairs (VA) had taken important steps to strengthen its computer security management program, including increasing security training; providing a more solid foundation for detecting, reporting, and responding to security incidents; and reducing the risk of unauthorized access through external connections to its critical systems. Nonetheless, the department had not yet fully implemented a comprehensive computer security management program that included a process for routinely monitoring and evaluating the effectiveness of security policies and controls and addressing identified vulnerabilities. Further, VA's offices were self-reporting computer security weaknesses, and the department lacked an independent component to ensure the accuracy of reporting and validating corrective actions taken.

[18] Office of the Inspector General, U.S. Department of Justice, *Independent Evaluation Pursuant to the Government Information Security Reform Act – Fiscal Year 2001 – Sensitive But Unclassified Systems*, Report Number 02-18, April 2002.

[19] U.S. General Accounting Office, *Information Security: Corps of Engineers Making Improvements, But Weaknesses Continue*, GAO-02-589 (Washington, D.C.: June 10, 2002).

- Department of Commerce officials have shown a commitment to correcting vulnerabilities identified in our August 2001 report.[20] They indicate that they have developed and implemented an action plan for strengthening access controls for the department's sensitive systems, published policy on comprehensive recovery plans which applies to all Commerce operating units to help ensure continuity of operations, and began the process of establishing a department-wide incident handling capability with formal procedures for preparing for, detecting, responding to, and reporting incidents. While neither the department's inspector general nor GAO has validated these corrective actions, these responses show that the agency is attempting to quickly address identified weaknesses.

Similar Control Weaknesses Continue Across Agencies

Although the nature of agency operations and their related risks vary, striking similarities remain in the specific types of general control weaknesses reported and in their serious adverse effect on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. Likewise, similarities exist in the corrective actions agencies must take. The following sections describe the six areas of general controls and the specific weaknesses that have been most widespread at the agencies covered by our analyses.

Security Program Management Controls

Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks in a cost-effective manner rather than reacting to individual problems in an ad-hoc manner only after a problem has been detected or an audit finding reported.

Despite the importance of this aspect of an information security program, poor security program management continues to be a widespread

[20] U.S. General Accounting Office, *Information Security: Weaknesses Place Commerce Data and Operations at Serious Risk,* GAO-01-751 (Washington, D.C.: Aug. 13, 2001).

problem. All the agencies for which this aspect of security was reviewed had deficiencies. As a result, these agencies

- were not fully aware of the information security risks to their operations,
- had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable,
- had a false sense of security because they were relying on ineffective controls, or
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

Establishing a strong security management program requires that agencies take a comprehensive approach that involves both (1) senior agency program managers who understand which aspects of their missions are the most critical and sensitive and (2) technical experts who know the agencies' systems and can suggest appropriate technical security control techniques. We studied the practices of organizations with superior security programs and summarized our findings in a May 1998 executive guide entitled *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our study found that these organizations managed their information security risks through a cycle of risk management activities that included

- assessing risks and determining protection needs,
- selecting and implementing cost-effective policies and controls to meet these needs,
- promoting awareness of policies and controls and of the risks that prompted their adoption among those responsible for complying with them, and
- implementing a program of routine tests and examinations for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action.

In addition, a strong, centralized focal point can help ensure that the major elements of the risk management cycle are carried out and serve as a communications link among organizational units. Such coordination is especially important in today's highly networked computing environments.

Implementing the cycle of risk management activities is the key to ensuring that information security risks are adequately considered and addressed on an ongoing, agencywide basis. Included within these risk management activities are several steps that agencies can take immediately. Specifically, agencies can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up to date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. Although none of these actions alone will ensure good security, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, these are steps that can be made without delay.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections—such as gates and guards—as well as logical controls, which are controls built into software that require users to authenticate themselves (through the use of secret passwords or other identifiers) and limit the files and other resources that authenticated users can access and the actions that they execute. Without adequate access controls, unauthorized individuals, including outside intruders and former employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Also, authorized users can intentionally or unintentionally modify or delete data or execute changes that are outside their span of authority.

For access controls to be effective, they must be properly implemented and maintained. First, an organization must analyze the responsibilities of individual computer users to determine what type of access (e.g., read, modify, delete) they need to fulfill their responsibilities. Then, specific control techniques, such as specialized access control software, must be implemented to restrict access to these authorized functions. Such software can be used to limit a user's activities associated with specific systems or files and keep records of individual users' actions on the computer. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and departing employees, as well as changes in users' responsibilities and related access needs.

Significant access control weaknesses that we have commonly identified include the following:

- Accounts and passwords for individuals no longer associated with an agency are not deleted or disabled or are not adjusted for those whose responsibilities, and thus need to access certain files, changed. As a result, in some cases, former employees and contractors could still (and in many cases did) read, modify, copy, or delete data; and even after long periods of inactivity, many users' accounts had not been deactivated.
- Users are not required to periodically change their passwords.
- Managers do not precisely identify and document access needs for individual users or groups of users. Instead, they provide overly broad access privileges to very large groups of users. For example, some operating system files were not protected from unauthorized access, permitting general users full access to these files. This would enable users to obtain passwords and system administration privileges, allowing a person to log in as someone else and use that access to read files, destroy or alter data, and initiate transactions.
- Use of default, easily guessed, and unencrypted passwords significantly increases the risk of unauthorized access. We are often able to guess many passwords on the basis of our knowledge of commonly used passwords and to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Vendors' default passwords or off-the-shelf parameters are used that do not meet the password requirements specific to the agency.

To illustrate the risks associated with poor authentication and access controls, in recent years we have begun to incorporate network vulnerability testing into our audits of information security. Such tests involve attempting—with agency cooperation—to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. In almost every test, our auditors have been successful in readily gaining unauthorized access that would allow both internal and external intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. Much of the activity associated with our intrusion testing had not been recognized and recorded, and the problem reports that were recorded did not recognize the magnitude of our activity or the severity of the security breaches we initiated.

Software Development and Change Controls

Controls over software development and changes prevent unauthorized software programs or modifications to programs from being implemented. Key aspects of such controls are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved before they are implemented, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes, and different versions are not misidentified.

Such controls can prevent errors in software programming as well as malicious efforts to insert unauthorized computer program code. Without adequate controls, incompletely tested or unapproved software can result in erroneous data processing that, depending on the application, could lead to losses or faulty outcomes. In addition, individuals could surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage.

Examples of weaknesses in this area include the following:

- Testing procedures are undisciplined and do not ensure that implemented software operates as intended. For example, fully developed procedures may not exist for controlling changes over software that would prevent unauthorized programs or modifications to an existing program to be implemented. Also, documentation is not always maintained to show that program changes have been tested, independently reviewed, and approved for implementation.

- Implementation procedures do not ensure that only authorized software is used. In particular, lack of adequate follow-up and documentation procedures for making emergency software changes increases the risk of software errors, which could cause system failures and/or data loss.

- Agencies' policies and procedures frequently do not address the maintenance and protection of program libraries. For example, the management software was not used to produce audit trails of program changes, maintain program version numbers, record and report program changes, maintain date information for production modules, and maintain copies of previous versions and control concurrent updates.

Segregation of Duties Controls

Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, a computer programmer should not be allowed to independently write, test, and approve program changes.

Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, improper program changes implemented, and computer resources damaged or destroyed. For example,

- an individual who was independently responsible for authorizing, processing, and reviewing payroll transactions could inappropriately increase payments to selected individuals without detection or
- a computer programmer responsible for authorizing, writing, testing, and distributing program modifications could either inadvertently or deliberately implement computer programs that did not process transactions in accordance with management's policies or that included malicious code.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Segregation of duties can be enforced by a combination of physical and logical access controls and by effective supervisory review. Common problems involve computer programmers and operators who are authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. An example of this would be a single individual authorized to independently develop, test, review, and approve software changes for implementation.

Operating System Software Controls

Operating system software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all applications that run on the system. Some system software can change data and program code on files without leaving an audit trail or can be used to modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Controls over access to and modification of system software are essential in providing reasonable assurance that security controls over the operating system are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosure. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues previously discussed. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them. A common type of problem reported is insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. Further, pervasive vulnerabilities in network configuration expose agency systems to attack. These vulnerabilities stem from agencies failure to (1) install and maintain effective perimeter security, such as firewalls and screening routers; (2) implement current software patches; and (3) protect against commonly known methods of attack.

Service Continuity Controls

The terrorist attacks that began on September 11, 2001, have redefined the disasters that must be considered in identifying and implementing service continuity controls to ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. Losing the capability to process, retrieve, and protect electronically maintained information can significantly affect an agency's ability to accomplish its mission. If service continuity controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete information. For some operations, such as those involving health care or safety, system interruptions could even result in injuries or loss of life.

Service continuity controls should address the entire range of potential disruptions including relatively minor interruptions, such as temporary power failures or accidental loss or erasure of files, as well as major disasters, such as fires or natural disasters, that would require reestablishing operations at a remote location. It is also essential that the related controls be understood and supported by management and staff throughout the organization. Senior management commitment is especially important to ensure that adequate resources are devoted to emergency planning, training, and related testing.

To establish effective service continuity controls, agencies should first assess the criticality and sensitivity of their computerized operations and identify supporting resources. At most agencies, since the continuity of certain automated operations is more important than others, it is not cost-effective to provide the same level of continuity for all operations. For this reason, it is important that management, on the basis of an overall risk assessment of agency operations, identify which data and operations are most critical, determine their priority in restoring processing, and identify the minimum resources needed to recover and support them. Agencies should then take steps to prevent and minimize potential damage and interruption. These steps include routinely duplicating or backing up data files, computer programs, and critical documents with off-site storage; installing environmental controls, such as fire suppression systems or backup power supplies; arranging for remote backup facilities that can be used if the entity's usual facilities are damaged beyond use; and ensuring that staff and other users of the system understand their responsibilities in case of emergencies. Taking such steps, especially implementing thorough backup procedures and installing environmental controls, are generally inexpensive ways to prevent relatively minor problems from becoming costly disasters.

Agencies should also develop a comprehensive contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. This plan should be documented, tested to determine whether it will function as intended in an emergency situation, adjusted to address identified weaknesses, and updated to reflect current operations. Both user and data processing departments should agree on the plan, and it should be communicated to affected staff. The plan should identify and provide information on supporting resources that will be needed, roles and responsibilities of those who will be involved in recovery activities, arrangements for off-site disaster recovery location[21] and travel and lodging for necessary personnel, off-site storage location for backup files, and procedures for restoring critical applications and their order in the restoration process. In testing the plan, it is most useful to simulate a disaster situation that tests overall service continuity, including whether the alternative data processing site functions as intended and whether critical computer data and programs recovered from off-site storage are accessible and current. Such testing not only helps managers identify weaknesses, it also assesses how well employees have been trained to carry out their roles and responsibilities in a disaster situation. Generally, contingency plans for very critical functions should be fully tested about once every year or two, whenever significant changes to the plan have been made, or when significant turnover of key people has occurred.

Contingency planning should also be considered within the larger context of restoring the organization's core business processes. Federal agencies depend not only on their own internal systems, but also on data provided by their business partners and services provided by the public infrastructure (e.g., power, water, transportation, and voice and data telecommunications). One weak link anywhere in the chain of critical dependencies can cause major disruptions to business operations. During the Year 2000 computing challenge, it was essential that agencies develop business continuity and contingency plans for all critical core business processes and supporting systems regardless of whether these systems were owned by the agency. As we reported in September 2000 on the lessons learned from this challenge, developing these plans was one of a number of management practices that, if continued, could improve federal agencies' overall information technology management, particularly in

[21] Depending on the degree of service continuity needed, choices for alternative facilities will range from an equipped site ready for immediate backup service, referred to as a "hot site," to an unequipped site that will take some time to prepare for operations, referred to as a "cold site." In addition, various types of services can be prearranged with vendors, such as making arrangements with suppliers of computer hardware and telecommunications services, as well as with suppliers of business forms and other office supplies.

areas such as critical infrastructure protection and security.[22] For example, in the aftermath of the attacks of September 11, 2001, news reports indicate that business continuity and contingency planning was a critical factor in restoring operations for New York's financial district, with some specifically attributing companies' preparedness to the contingency planning efforts begun for the Year 2000 challenge.

Despite this increased focus on business continuity and contingency planning, our analyses show that most federal agencies currently have service continuity control weaknesses. Examples of common agency weaknesses include the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.
- Disaster recovery plans were not fully tested to identify their weaknesses. For example, agencies had not performed periodic walkthroughs or unannounced tests of the disaster recovery plan—tests that provide a scenario more likely to be encountered in the event of an actual disaster.

GISRA Spurs Agency Actions, But Highlights Weaknesses

As we reported in March 2002, first-year GISRA implementation demonstrated that the new law provides a significant step in improving federal agencies information security programs.[23] To implement GISRA requirements and comply with OMB guidance, agencies reviewed their information security programs, reported the results of these reviews and their IGs' independent evaluations to OMB, and developed plans to correct identified weaknesses. In addition, GISRA implementation has also resulted in important actions by the administration, which if properly implemented, should continue to improve information security in the federal government. For example, OMB has issued guidance that information technology investments will not be funded unless security is incorporated into and funded as part of each investment. Administration actions and plans also include

[22] U.S. General Accounting Office, *Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges,* GAO/AIMD-00-290 (Washington, D.C.: Sept. 12, 2000).

[23] GAO-02-470T.

- directing all large agencies to undertake a review to identify and prioritize critical assets within the agencies and their interrelationships with other agencies and the private sector, as well as a cross-government review to ensure that all critical government processes and assets have been identified;
- integrating security into the President's Management Agenda Scorecard;
- developing workable measures of performance;
- developing e-training on mandatory topics, including security; and
- exploring methods to disseminate vulnerability patches to agencies more effectively.

Other actions include additional security guidance by OMB and NIST. For example, OMB has provided the agencies with specific performance measures for agency officials who are accountable for information and information technology security and required the agencies to report actual performance for these measures in their fiscal year 2002 GISRA reports. Further, NIST-developed guidance includes a Security Self-Assessment Guide and supporting tools to help agencies perform self-assessments of their information security programs.[24] This guide accompanies NIST's Security Assessment Framework methodology, which agency officials can use to determine the current status of their security programs.[25] The guide itself uses an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. Many agencies used a draft version of the self-assessment guide for their fiscal year 2001 GISRA program reviews, and with issuance of a final version in November 2001, OMB now requires that the guide be used for fiscal year 2002 reviews. Also, NIST developed a tool to automate completion of the guide's questionnaire that can be found at its Computer Security Resource Center web site: http://csrc.nist.gov/asset/.

In addition to these actions, the actual results of GISRA reviews and evaluations have helped to further highlight where agencies have not established information security programs consistent with GISRA

[24] National Institute of Standards and Technology, *Security Self-Assessment Guide for Information Technology Systems*, NIST Special Publication 800-26, November 2001.

[25] National Institute of Standards and Technology, *Federal Information Technology Security Assessment Framework*, prepared for the Federal CIO Council by the NIST Computer Security Division Systems and Network Security Group, Nov. 28, 2000.

requirements and where significant weaknesses exist. In its fiscal year 2001 report to the Congress on GISRA, OMB noted that although examples of good security exist in many agencies, and others are working very hard to improve their performance, many agencies have significant deficiencies in every important area of security.[26] In particular, the report highlights six common security weaknesses: (1) a lack of senior management attention to information security; (2) inadequate accountability for job and program performance related to information technology security; (3) limited security training for general users, information technology professionals, and security professionals; (4) inadequate integration of security into the capital planning and investment control process; (5) poor security for contractor-provided services; and (6) limited capability to detect, report, and share information on vulnerabilities or to detect intrusions, suspected intrusions, or virus infections.

Our analyses of the results of agencies' fiscal year 2001 GISRA reviews and evaluations also showed that agencies are making progress in addressing information security, but that none of the agencies had fully implemented the information security requirements of GISRA and all continue to have significant weaknesses. In particular, our review of 24 of the largest federal agencies showed that agencies had not fully implemented requirements to

- conduct risk assessments for all their systems;
- establish information security policies and procedures that are commensurate with risk and that comprehensively address the other reform provisions;
- provide adequate computer security training to their employees, including contractor staff;
- test and evaluate controls as part of their management assessments;
- implement documented incident handling procedures agencywide;
- identify and prioritize their critical operations and assets and determine the priority for restoring these assets should a disruption in critical operations occur; or

[26] Office of Management and Budget, *FY 2001 Report to Congress on Federal Government Information Security Reform* (February 2002).

- have a process to ensure the security of services provided by a contractor or another agency.

According to OMB's July 2002 guidance, agencies and their IGs were required to submit the results of their fiscal year 2002 GISRA reviews and evaluations to OMB by September 16, 2002, and to submit corrective action plans by October 1. Our most recent analyses of audit reports and evaluations to identify significant information security weaknesses considered the results of the IGs' fiscal year 2002 GISRA independent evaluations. In addition, in response to a request by this subcommittee, we are currently evaluating the results of agencies' second-year GISRA implementation; our evaluation is to include an analysis of agencies' corrective action plans and their progress in correcting identified weaknesses.

At this time, however, GISRA is still scheduled to expire on November 29, 2002. And although several bills would address GISRA reauthorization, none have yet been enacted. We believe that continued authorization of such important information security legislation is essential to sustaining agencies' efforts to identify and correct significant weaknesses. Further, this authorization would reinforce the federal government's commitment to establishing information security as an integral part of its operations and help ensure that the administration and the Congress continue to receive the information they need to effectively manage and oversee federal information security.

Improvement Efforts Are Underway, But Challenges Remain

Information security improvement efforts have been undertaken in the past few years both at an agency and governmentwide level. These efforts include the agency, IG, and OMB actions to implement GISRA information security requirements and correct identified information security weaknesses. In addition, in October 2001, President Bush signed executive orders creating the Office of Homeland Security and establishing the President's Critical Infrastructure Protection Board.[27] Chaired by the Special Advisor to the President for Cyberspace Security, the board is to coordinate cyber-related federal efforts and programs associated with protecting our nation's critical infrastructures and recommend policies

[27] "Establishing the Office of Homeland Security and the Homeland Security Council," Executive Order 13228, October 8, 2001 and "Critical Infrastructure Protection in the Information Age," Executive Order 13231, October 16, 2001.

and coordinating programs for protecting information systems related to critical infrastructure protection. In addition, the board is intended to coordinate with the Office of Homeland Security in activities relating to the protection of and recovery from attacks against information systems for critical infrastructure.

In July 2002, the President also issued the National Strategy For Homeland Security to "mobilize and organize our nation to secure the United States homeland from terrorist attacks."[28] According to the strategy, the primary objectives of homeland security in order of priority are to (1) prevent terrorist attacks within the United States, (2) reduce America's vulnerability to terrorism, and (3) minimize the damage and recover from attacks that do occur. This strategy also calls for the Office of Homeland Security and the President's Critical Infrastructure Protection Board to complete cyber and physical infrastructure protection plans, which would serve as the baseline for developing a comprehensive national infrastructure protection plan. While the national strategy does not indicate a date when the comprehensive plan is to be completed, in September 2002, the board released a comment draft of a National Strategy to Secure Cyberspace.[29] Defined as a strategy of steps the United States will take to secure the information technology networks necessary for the nation's economy, defense, and critical services to operate, the strategy is divided into five audience levels ranging from home users and small businesses to discussion of global issues. Level 3 describes the issues and challenges of, and makes recommendations for, critical sectors, including the federal government, state and local government, higher education, and the private sector.

These actions are laudable. However, given recent events and reports that critical operations and assets continue to be highly vulnerable to computer-based attacks, the government still faces the challenge of ensuring that risks from cyber threats are appropriately addressed. Accordingly, it is important that federal information security efforts be guided by a comprehensive strategy for improvement.

We believe that the following seven steps should be taken as part of a comprehensive strategy for improvement.

[28] Office of Homeland Security, the White House, *National Strategy for Homeland Security,* July 2002.

[29] The President's Critical Infrastructure Protection Board, *The National Strategy to Secure Cyberspace—For Comment Draft,* September 2002.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security. This strategy should also consider other organizations with information security responsibilities, including OMB, which oversees and coordinates federal agency security, and interagency bodies like the CIO Council, which are attempting to coordinate agency initiatives. It should also describe how the activities of these many organizations interrelate, who should be held accountable for their success or failure, and whether they will effectively and efficiently support national goals.

Second, more specific guidance to agencies on the controls that they need to implement could help ensure adequate protection. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which to enforce these controls. In theory, this discretion is appropriate since, as OMB and NIST guidance states, the level of protection that agencies provide should be commensurate with the risk to agency operations and assets. In essence, one set of specific controls will not be appropriate for all types of systems and data. Nevertheless, our studies of best practices at leading organizations have shown that more specific guidance is important.[30] In particular, specific mandatory standards for varying risk levels can clarify expectations for information protection, including audit criteria; provide a standard framework for assessing information security risk; help ensure that shared data are appropriately protected; and reduce demands for limited resources to independently develop security controls. Implementing such standards for federal agencies would require developing a single set of information classification categories for use by all agencies to define the criticality and sensitivity of the various types of information they maintain. It would also necessitate establishing minimum mandatory requirements for protecting information in each classification category. At this time, NIST plans to publish a special publication in Spring 2003 that establishes a set of standardized, minimum security controls for information technology systems addressing low, moderate, and high levels of concern for confidentiality, integrity, and availability.

Third, ensuring effective implementation of agency information security and critical infrastructure protection plans will require active monitoring by the agencies to determine if milestones are being met and testing to determine if policies and controls are operating as intended. Routine periodic audits, such as those required by GISRA, would allow for more

[30] U.S. General Accounting Office, *Information Security Management: Learning from Leading Organizations*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

meaningful performance measurement. In addition, the annual evaluation, reporting, and monitoring process established through GISRA is an important mechanism, previously missing, to hold agencies accountable for implementing effective security and to manage the problem from a governmentwide perspective.

Fourth, the Congress and the executive branch can use audit results to monitor agency performance and take whatever action is deemed advisable to remedy identified problems. Such oversight is essential for holding agencies accountable for their performance, as was demonstrated by OMB and congressional efforts to oversee the Year 2000 computer challenge.

Fifth, agencies must have the technical expertise they need to select, implement, and maintain controls that protect their information systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. Highlighted during the Year 2000 challenge, the availability of adequate technical and audit expertise is a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their information security and infrastructure protection activities. In our review of first-year GISRA implementation, we reported that many agencies emphasized the need for adequate funding to implement security requirements, and that security funding varied widely across the agencies. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, additional amounts are likely to be needed to address specific weaknesses and new tasks. At the same time, OMB and congressional oversight of future spending on information security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes that are not supported by a strong agency risk management process. Further, we agree with OMB that much can be done to cost-effectively address common weaknesses, such as security training, across government rather than individually by agency.

Seventh, expanded research is needed in the area of information systems protection. While a number of research efforts are underway, experts have noted that more is needed to achieve significant advances. In addition, in its December 2001 third annual report, the Gilmore Commission recommended that the Office of Homeland Security develop and implement a comprehensive plan for research, development, test, and evaluation to enhance cyber security.[31] In this regard, the Congress recently passed the Cyber Security Research and Development Act (H.R. 3394) to provide $903 million over 5 years for cybersecurity research and education programs. This bill, which has been sent to the President for signature, would direct the National Science Foundation to create new cybersecurity research centers, program grants, and fellowships. It would also direct NIST to create new program grants for partnerships between academia and industry.

Mr. Chairman, this concludes my written testimony. I would be pleased to answer any questions that you or other members of the Subcommittee may have at this time.

If you should have any questions about this testimony, please contact me at (202) 512-3317. I can also be reached by e-mail at daceyr@gao.gov.

(310180)

[31] *Third Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction* (Dec. 15, 2001).

Mr. HORN. The vice chairman, Mr. Lewis, would like to take a look at some of these, and I want him here because he's the only member of this full committee and the subcommittee of Ways and Means. That's a very lofty committee and goes back to the first—1789. And they also have to do with tax administration. And I'm hoping with him being on Ways and Means that we can get our debt collection law, which Mrs. Maloney and I put together in 1996—and it's going great right now. It's just that's for nontax. And now we'd love to have you, Ron, as the—if you can sneak in at night to get them to get the debt collection.

And when I looked at that—and that's when I asked the then-President, how about getting a CEO, because we're not getting anywhere, and IRS in one pot had $100 billion sitting there to be collected. When I counseled that one, they said, Oh, oh, there's one other one, easier; $60 billion. And we're looking for money in this country? Let's get it done. And you will be a hero, Ron. And good luck.

Mr. LEWIS. Thank you, Mr. Chairman. We could use some extra money right now.

Mr. HORN. Yep.

Mr. LEWIS. Mr. Forman, the OMB has issued guidelines stating that agencies must include security procedures in their budget requests for information technology projects. They do not—the OMB has said it will not fund the project. Has the OMB refused any funding for this reason?

Mr. FORMAN. Yes, we did last year. There will of course be some more feedback we'll give to the agencies. Generally the approach—and we do this with a business case—is to refuse funding if an agency does not have good justification on a number of the components, security being one of them.

There are a number of programs last year that we put on the high-risk list for fiscal year 2003 where security was the predominant problem, and so we spent quite a few months working with the agency to address the security problems. I'd say generally—I can't say for a fact it's in every case—but generally the agencies would rather work through their security problems than not get funding, so that incentive structure seems to work.

Mr. LEWIS. Very good. Thank you.

Excuse me, I get the opportunity to give you some more questions. The Security Act requires that agency corrective action plans address all known vulnerabilities. If agency plans fail to include all known vulnerabilities, what action will the OMB take?

Mr. FORMAN. We, through both last year's guidance and then this year's most recent guidance, have taken a comprehensive approach. That's one of the reasons that we believe so strongly in having both a CIO's report and an audit followup process leveraging the IGs. The ultimate approach, therefore, when we get the reports and the submission is to compare the two sets of data. Also use the GAO data and work via the budget process to ensure that remediation occurs.

Lets say, as I pointed out in my testimony, one of the recurring problems that we've seen is agencies' desires to invest in new IT and at the same time claim that they can't remediate legacy systems problems. There's a tradeoff to be made. Obviously, if a legacy system is only going to exist for 5 or 6 months, one may not invest in a total security overhaul, and there are other ways to protect the system. But there are too many instances still where we see agencies not doing what I consider the nuts and bolts here.

A corrective action plan has to include some certification and accreditation of the legacy systems. And so again we are making very clear to the agencies that we're simply not going to fund new investments and short remediation on accreditation certification. I think you'll see that's a much bigger focus this year for us when the report comes in in the February timeframe.

Mr. LEWIS. Based on the OMB's analysis if the performance measures required in the Government Information Security Reform Act Report, it accurately measures the agency's progress in securing their critical computer systems. Does it?

Mr. FORMAN. The—I think there are a couple of issues to consider. First of all, I'd say yes; but it's at a high management level. And, of course, one of the things that the chairman has worked so hard on for many years I think is coming to fruition. We've got secretaries and deputy secretaries now who are focusing on security. In fact, within the White House, all the way up to the President, people are focused on cyber security now. There's a difference, though as we get into the details. And I think as my colleague from GAO has laid out very clearly, it's time to get into the nuts and bolts. And program management now comes much more to the forefront.

So we too are going to shift our focus on that and onto a lot of nuts and bolts. At the same time, I don't think you can ignore the fact that the vulnerability and threat picture has shifted. So there are a couple of types of threats. One, I would consider the hacker threat that we addressed in the testimony. And in there we're making much heavier reliance on FedCert and increasing their capabilities, the patch management services contract that I alluded to. And by leveraging XML and some of the easier reporting technologies to reduce the burden and literally allow for electronic-type reporting of incidents so you don't have to have a person in the process per se, we can make that a seamless process and we'll move forward in that.

The organized threats are going to take a different level of response and a different approach to that, I think, than what we're viewing in hackers. While I can't get into, obviously, much of the discussions going on, I think you're probably aware that the deadline for comments on the cyber strategy is today. But what I can say is that regardless of what happens, we know we have to tighten up the continuity of business operation planning again, as Mr. Dacey alluded to. It's better, but this is very similar to the Y2K issue. And before September 11 last year, I'd say very few of the agencies had been maintaining the continuity of operations plan. So that too has become a big focus for us.

Mr. LEWIS. One more question. The OMB's 2001 Report to Congress required by the Government Information Security Reform Act highlighted six common weaknesses of Federal agencies. Have you noted any significant improvements in these areas?

Mr. FORMAN. As I alluded to in my testimony, yes, although it's not as governmentwide as we would like to see in all the areas.

Some agencies are making marked progress. We have some discrepancies based on our initial view, versus the chairman's scorecard. But what I'd say is that the most marked increase is in the senior manager, the secretary and deputy secretary focus, and that, without a doubt, is uniform now across the board, as I think you heard from Deputy Secretary Lockhart and also others on the panel.

Mr. LEWIS. Thank you.

Mr. HORN. Thank you. Let's talk about Commissioner Lockhart's work and how that goes about. And would it be possible, Mr. Forman, that OMB might have various types of teams brought together of different Cabinet departments so that you could go out—and the word "accreditation" was mentioned a little while ago. And if we had a team like that needed some help, would that be useful to OMB?

Mr. FORMAN. Well, there are some teams in the Federal Government that do get involved in a range of security reviews: obviously, the National Institution for Standards and Technology, Department of Energy, and I believe some other departments. There's a fruitful source of this support in the private sector. The Interior Department, for example, has engaged a company to help them with accreditation and certification. This capability is a type of service that is exactly as you laid out. It's project based. It's team based. And I don't know that it's inherently governmental. There are clearly a set of government rules and regulations, but they're also industry practices. It gets down to things like what's the proper way to install a certain type of software or a certain server; is it outside or inside the firewall? And my preference would actually be that rather than buildup huge teams within the government that were forever trying to work across traditional silos, that we would increase our reliance or continue our reliance on the private sector teams. I know that companies, as us, have a growing demand for that type of service.

Mr. HORN. Commissioner Lockhart, would you be willing to let some of your best people for a while go in other parts of the executive branch?

Mr. LOCKHART. Well, Mr. Chairman, we do have some very good people and we have some very big challenges. Now, would we very much like to work with the rest of the government and we're trying to, through mechanisms like the President's Management Council which I serve on, trying to go across government and work together.

I guess I would agree with Mr. Forman that—and we use this extensively. We use a lot of private sector expert technology and consulting firms to do this kind of activity. We work with them. We would be happy to share our expertise, but we have a lot of needs. Even though we have good grades from you, we still have a long ways to go. So I would like to keep them internally, if we could.

Mr. HORN. Well, I can realize that. But it seems to me, you don't have to do it all the years, but get in there and help them.

Mr. LOCKHART. Well, certainly we are involved in the CIO group. We do share best practices, and we will continue to do that. We learned from other departments, and hopefully they learned from us.

Mr. HORN. With Social Security and with your being on the council—aren't you? And that includes all CIOs?

Mr. LOCKHART. Well, the council I referred to is President, Managing Council, which is the Deputy Secretary, Deputy Commissioner.

Mr. HORN. And that is your equivalent for Social Security?

Mr. LOCKHART. Right.

Mr. HORN. And what I am wondering about, when I hear there is no CIO in one place, Mr. Forman, do we have any more that are missing CIOs?

Mr. FORMAN. Departments that are missing CIOs?

Mr. Horn. Yes.

Mr. FORMAN. Yes, we do. I thought we had gotten a full cadre, but we seem to run up against the inevitable situation in government where people stay in new jobs for around 18 months. And so we are working through getting some new folks.

What I would say is that we do seem to get good talent in these jobs, as people are retiring or leaving for other opportunities, finding good people to fill in; and I will give you an example on that. I think one of the most important ones here is the security liaison in the CIO counsel, and that's a CIO that essentially works with the different committees—we have three major committees, the Workforce Skills, the Best Practices Committee, and the Architecture Committee—and fuses security focus into those committees.

Ron Miller, who had been the CIO at FEMA, moved over to work on the transition team. FEMA was able to promote a deputy that he had recruited, a very talented and capable person, Rose Parks, to their C IO. But meanwhile, we quickly, because of the importance of this, wanted to make sure we had a solid CIO for that liaison, and so we picked Van Hitch, who is the CIO at the Justice Department.

Now, Justice is—one of the differences of opinion I would have with your scorecard, I think they made good progress there. But Van also was a recent hire from the private sector. When he was hired into the government, he came in with—and this was one of the early ones—Attorney General anointing the CIO as having the responsibility that was originally envisioned under the Klinger-Cohen Act.

So we are working through the inevitable rotation, and there are some success stories there as well.

Mr. HORN. Now, CFOs, are we short them in some of the agencies and departments?

Mr. FORMAN. That, I am not prepared to address.

Mr. HORN. Anybody here looking, stealing people from one place to the other? Well, let us get it in the record; and, without objection, it will be put in at this point.

I would just like to know the degree to which Chief Financial Officers, what relation do they have to help in this situation and work with the Chief Information Officer? And I would like to hear how that—because part of the problem here is who is getting what part of the pie to get the cyber situation.

Mr. LOCKHART. I can answer from the Social Security standpoint. I think we find that working relationship extremely important between the CFO, the CIO, and the Systems Group. And they work very closely; they are all part of the senior management team of Social Security. We work closely in a very integrative fashion on the budget process; we work on the fiscal security, as well as computer security, together. And I think that teamwork has really helped and been part of our success, in that we have people extremely devoted to the agency and to our mission; and, you know, partially that is because since almost day 1 of Social Security, we have been concerned about personal security, personal privacy. That was our first regulation. And so it is really infused in our culture, and that includes the CFO, the CIO, the Systems Group, and really the 65,000 people of Social Security.

And so that is one of the important ways that we have tackled this.

Mr. HORN. I was heading just for you, the Inspector General. And you have got a council, too. And so what is happening that IGs, you are doing, for example on the financial management part of your working? You are the one that can go outside and put in the accounting aspects of it, and I would be curious how much the I Gs can help the C IO so they can get the resources they need.

Mr. MEAD. I think the Inspector General concept is really key to helping both the CIO and the CFO functions fully blossom. And the creatures we call Inspectors Generals, have a very peculiar reporting relationship. By law, we are to report to the Secretary and the Congress to keep each currently and fully informed.

Inspectors Generals are that part of the agency that are responsible for auditing. They see things happening much earlier than other outside oversight agencies might be able to; and you are able to effect proactive change. And I think that it is important that you have a collaborative relationship with the CIOs and CFOs in these agencies.

And I would say, for example, that in the Department of Transportation, the CFO is also the Assistant Secretary for Budget, which means that CFO has clout. When the Assistant Secretary for Budget speaks, she is also speaking with her CFO hat.

We have turned the situation around on the financial statements at DOT. For almost 8 or 9 years running, they got a disclaimer, and now they have greatly improved their financial situation.

The situation with the Chief Information Officer is a bit different because the Chief Information Officer doesn't have any line authority over much of anything. And I point that out in contradiction to the Chief Financial Officer construct.

Mr. FORMAN. If I can add to that, I think that it is important to understand the implications there on a couple of fronts.

First of all, when we talk about the President's management agenda and the five scorecards, there are a lot of interrelationships, and the one that is important here is between the financial management scorecard and the e-government score. Generally—and we went through this in this last quarter—when there is a material weakness related to the security program, the agency is going to get a double zinger. They will get it on the management scorecard and they will get it on the e-government scorecard.

What the public sees is the scores. What the President sees is the detail behind the scores, and that includes the name of the person who is responsible for it. So they will see the zinger on the two scores with the CIO, or whoever the e-government lead is for that department; and the CFO, or whoever is the financial management lead for that department.

It is important, therefore, I think, that we continue to have computer security linked with being a financial material weakness.

The other thing that you alluded to, though we did go through this almost a year ago, a situation where a CFO said, Oh, OMB will forget about the security issues; it is not a big deal. And that CFO learned that was a career-threatening comment. This is extremely important to the White House. And that—I think that word has gotten around to the other CFOs now.

Mr. HORN. There is a CFO in the executive forces of the executive branch where OMB is there and a whole group of agencies. Is that CFO still there?

Mr. FORMAN. That is a good question. Again, I don't know for a fact that person is still in their job.

Mr. HORN. Well, we put it in there before the current President, and it was—we tried to do it with the previous President. And they said no, no, we don't want that. And I said, hey, wait a minute. This will be for the next President. Oh, no problem, they said, let them do it. Good heavens.

Now, I am just curious, because we do need a CFO and a CIO. Now, who is the CIO that helps your colleagues in the executive office of the President?

Mr. FORMAN. Well, I am not sure that we have the formal or—the formal anointment of a CIO. Our CIO, who had been your CIO here in the House, was promoted to the Office of Administration. So his deputy moved up as at least the acting CIO. And I think—as you know, we have worked fairly closely with the Appropriations staff to make sure that the executive office of the President is being held to the exact same standard that we are holding all the other agencies to. That is a commitment. You know, if you are going to hold other agencies accountable, you have to start by holding yourselves accountable. So we have done that.

I will say that—and I don't know our results on our security review yet, but I will say, as the user, primary user, I have had more things stripped from e-mails by our firewall, which is one of the signs I know. We don't experience many—much down time. And we are ultimately a prime target in the hacker community. So we have extensively strong firewalls and an exceedingly risk-adverse IT security policy that is employed to fight firewalls and other tools.

Mr. HORN. Is there a question on this particular?

Mr. LEWIS. No.

Mr. HORN. Go ahead.

Mr. LEWIS. There is one question that I wanted to get to, and I have to leave in just a second.

Mr. Mead, the Federal Aviation Administration, does the Federal Aviation Administration have a tested contingency plan to ensure that it can continue to operate its air traffic control system if hackers were to successfully attack? That is important to all of us.

Mr. MEAD. I will give this in a two-part answer.

First, a decision was made earlier this year, based on a report we issued, with recommendations that the air traffic control system would not be tied in any way to the Internet. There was a proposal from FAA that has been percolating from 1999 to 2000 period that they would have a system that, in theory, would be insulated from the Internet, but we felt it would be vulnerable.

A high-level decision was made this year, that would not be the case. Therefore, the air traffic control system cannot be hacked through directly from the Internet. And I think that was a very good decision; although it is going to cost some money, it is worth it.

Second, the air traffic control system, if one part of it were to go down for some reason, other elements of it can pick up the operations for a short period of time. We do think, as reported in our GISRA report, that for the longer term FAA needs a more robust contingency plan. But for the shorter term, we think they have a good one.

In addition, as I noted in our testimony, the background checks on people have improved dramatically over the last couple of years. The principal exposure we have on the AT C system is not from private attackers; it is insiders or contractors. That is where the attention needs to be focused.

But for the short term, I can give you good assurances that we are in decent shape. For the longer term, we need to pay more attention. And that is what we reported to OMB and the Secretary.

Mr. LEWIS. Thank you.

Thank you, Mr. Chairman.

Mr. HORN. Thank you. Appreciate it.

Let us just have a couple with Mr. Mead, the Inspector General. And the Security Act directs the agency's Chief Information Officer to develop and maintain an agency-wide information security program; yet, the Department of Transportation has not had a Chief Information Officer since January 2001.

Why has this been allowed to continue, and who has taken on the responsibility in lieu of the Chief Information Officer?

Mr. MEAD. Why has it happened? It has not been for want of recruiting. They did have a candidate; that fell through for one reason or another. They are now vetting other candidates. But I have got to say that I think that the importance of the position needs to be recognized more vigorously. If you were talking about the FAA Administrator, the Assistant Secretary for Budget, or the Deputy Secretary, those positions would not be allowed to go vacant for such a long period of time.

We will have a Chief Information Officer. I think it will take probably 2 or 3 more months. But we really need one.

You know, this year, Mr. Chairman, OMB did something I think was quite good. They brought together the management side of OMB, the budget side, at very senior levels—the Inspector General, the budget people, the Chief Financial Officer. And they went over their range of material weaknesses that needed to be addressed. And missing, of course, was our Chief Information Officer because we didn't have one.

Instead—and here is the answer to the second part of your question—we had the acting Chief Information Officer who has taken on that position frequently, given that over the last 6 years we have had a Chief Information Officer for only 18 months.

Mr. HORN. And you haven't seen a problem. Is that it? Or——

Mr. MEAD. No. I have seen a problem, and the problem is two fold at DOT. One, the CIO does not have line authority over budgets. Two, the CIO does not have input into the performance appraisals of the Chief Information Officers of the various operating administrations. You need to have those two elements.

We did have a Chief Information Officer for 18 months during the last administration, and we still had problems. We had problems largely because the operating administrations did not feel accountable to that CIO. And right now you have Secretary Mineta and Deputy Secretary Jackson doing the street work to get attention paid to information security. And they are doing a good job, but they have a lot of other things to do, too.

Mr. HORN. Mr. Forman, are there other CIOs that do not have any—looking at, in terms of the budget? Or is it at the upper level of the Deputy Secretary?

Mr. FORMAN. Well, obviously, especially in this era we want the secretaries and deputy secretaries to focus on improving the quality of the cyber security posture at the departments.

But I have to agree with Mr. Mead; where we have seen progress, there has been clear action taken to empower the CIO. We did some of that in the budget process last year. Obviously, our focus on capital planning and enterprise architectures is specifically for that purpose, but also other Secretaries, the Attorney General. So, where there is a Secretary or where we are working with the Secretaries make it clear that the CIO is fully empowered, we see progress.

Now, I would say transportation is one where there is a less-than-powerful CIO. I think, though, we have—whether it is OMB or if you talk to the Secretary or Deputy Secretary, all agree they need a powerful CIO. You run into an interesting situation then, trying to recruit someone, because you know that first person there is going to be one that is going to take on some very longstanding cultural issues, political issues, both internal and relationships between operating administrations and the Congress. And it does take, I have found, a concerted effort in working with this committee, with the Appropriations committees, with the leadership of that department and OMB, to make that change occur. And that is really tough absent a burning document or crisis like the situation at Interior.

Mr. HORN. Well, we will move to the Carnegie Mellon expert here. And in your testimony, you state that the number of reported incidents continues to rise. Mr. Mead stated that the Department of Transportation has reported more than 25,000 incidents in 2002, although all may not have been intrusions. Meanwhile, some agencies, such as the Department of Housing and Urban Development, have reported no incidents.

Given your expertise on this subject, how would you explain this disparity?

Mr. PETHIA. Two reasons that I can think of. One of them is that often organizations, both in the government and in the private sector, shy away from reporting incidents because they don't want the little black mark that goes next to their name that says there is a possibility of a security problem. We certainly see a lot of that in the private sector. Concerns over loss of confidence in the organization make people reluctant to want to report.

The second reason is that very often I think a lot of these incidents go not just unreported but undetected. We know that intrusion detection technology is only moderately effective. We know that many organizations don't have active programs in place to monitor their systems and monitor their networks to look for signs of intrusion.

So I think it is a combination of both, organizations that don't want to report because they are concerned about embarrassment, but also, all too often, the case that these incidents go undetected.

Mr. HORN. You expressed concern about the vulnerabilities associated with the supervisory control and data access systems. Can you give us a specific example of the result if one of these systems which controls some of the Nation's critical infrastructure were successfully attacked?

Mr. PETHIA. The example that was in my testimony was a case that was reported from Australia where it was actually a disgruntled employee who decided to affect the operations of a sewage control system, and in fact, hundreds of thousands of gallons of sludge were dumped out into the environment causing the environmental impact of that. You can hypothesize certainly other kinds of incidents where, very simply, things like oil stops flowing, natural gas stops flowing, power isn't delivered to certain parts of the country, hydroelectric dams are suddenly releasing water into river valleys where the level of water is not expected.

So I think this is an area where we have to begin to understand and pay more attention to the fact that the cyber world and the physical world are now tightly connected. And we often think about physical events and cyber events as separate kinds of things, but now that we are living in a situation where we have to pay attention to terrorists, people that want to disrupt our society, I think we have to, all of us, have a better understanding of how the cyber world and the physical world are connected, how physical attacks—how the impact of those attacks can be amplified by cyber attacks. So, for example, if there were to be a physical attack on one of our cities disrupting the communications systems that, at the same time, would slow the response to that kind of an attack, it would slow emergency services.

And similarly, we can see how physical attacks can exacerbate the cyber attacks as well. And that is an area of work that I think—you know, now that we are beginning to get some of the basics in place, I think we need to look beyond just cyber alone and look at the connection between cyber and physical.

Mr. FORMAN. Mr. Chairman, if I may address a key point in that. You know, we track data on intrusions, and we see the numbers of thousands of intrusions. And while I am sure that is important, the issue that has long existed is the internal threat. And the corollary to that is, you have to know what you do once you intrude. You have to know what a piece of data is. Breaking into an Oracle or an I BM DB2 data base doesn't get me anywhere if I don't have a copy of that somewhere on my computer and know what that data structure is. Otherwise, all I have done is revealed a string of, who knows what.

So it is not as—I don't believe, as simple as saying the number of intrusions have gone up and therefore there is a real problem here. You have to have some insight about what you are doing in order to say there is a real vulnerability or threat.

Mr. HORN. Any thoughts on that comment?

Mr. PETHIA. I think that is certainly true. The great majority of what we see out there are what I often call "recreational hacking attacks," hackers are out looking for things to explore or out to prove some kind of a political point who are not really bent on doing damage. But I think as we become more reliant on this technology and as we interconnect more and more of our systems, the people who are serious about causing damage, or the people who are serious about taking advantage of us for their personal profit, the criminals and the terrorists, will begin to move more and more into this space.

And I agree with Mark, you certainly can't attack a system and do an awful lot of damage unless you do know something about it. But we do know that our systems are being surveilled, we know that they are constantly being probed, we know that networks are being mapped. We know that there are people out there who are working very hard to understand how our systems are configured and how they are put together. And so I think a lot of the thing we have to pay attention to is the insider threat. But an awful lot of outsiders are working hard to become as knowledgeable as the insiders, and we can expect to see those kinds of attacks in the future.

Mr. HORN. Well, along that line of someone with your extensive knowledge of Federal operations, what are the most important actions Federal agencies must take to improve their computer security?

Mr. PETHIA. I am very happy to see GISRA and the effects that it is beginning to have. I think the steps that are outlined there are exactly the right ones for agencies to go through right now. But as Mark said, Mr. Forman, earlier in his testimony, as we are now beginning to get some of these high-level things in place, it is time to get down into the details, the nuts and the bolts.

And that is why I often speak about the need for more trained professionals, more knowledge about security, security issues, because this risk management action—as we begin to get the senior level attention, as we begin to get security plans in place, as we begin to go through an annual process, now it is time to implement those corrections that are needed; and that requires knowledgeable people. And so I think the next step is for agencies to have a real understanding of exactly why these vulnerabilities are serious, and then to put into effect the right kind of implementations and monitor those implementations for effectiveness over time.

Mr. HORN. Mr. Dacey, based on your analyses of the last 2 years of agency reports required by the Government Information Security Reform Act, do you believe that the Federal Government is making progress in its efforts to secure the government computer systems?

Mr. DACEY. Yes, Mr. Chairman, I do believe they are making progress. There are many actions under way both, as I said, at a governmentwide level and agency level; and I would distinguish some of those actions. I think some of them were challenging, but longer-lasting actions will take some time to fully implement. We have talked about some of these here this morning.

Putting in an effective security management program, I think is key, because oftentimes in doing our audits, we find that maybe the agency in fact fixed some of the specific weaknesses on the specific systems we audited, which is only a small portion of the agency systems, and yet we find the same types of incidents and problems occurring in other systems within the agency; and in fact have seen on several occasions the same weaknesses occur as new operating systems are installed and the same changes aren't made to those new operating systems that were fixed on the old ones.

So I do think security management is key. I think we are seeing some fundamental changes taking place. We talked earlier today, the Honorable Mr. Lockhart had talked about SSA and their efforts to monitor their systems and put together a program to really highlight to executive management what is going on and really to probe their own systems and understand; and we are seeing some efforts in that arena as well.

We are seeing responsibilities changing—VA recently moved the responsibilities for security and all of the budget decisions to the CIO similar to what we talked about. And I know there are a number of agencies, although I don't know which today, that is still an issue—but we have seen where that is happening, it is starting to make fundamental changes to the core, because what we really need is a structure of management that can address these problems.

We talk about vulnerabilities that are showing up with a magnitude of about a 12 or 13 a day, on average, and I am sure that is increasing. Mr. Pethia might update us on that. But it really calls for a fundamental structure; and it is a management challenge rather than a technical one.

I do agree we need to address some of the technical issues. I think with the bill that Congress recently passed to provide some funding for research and development and education are two key areas that will help address some of those problems. But—I do think those are the issues, but I do think there are improvements. I think there need to be more, though.

And again getting back to the other discussion, some of the nuts and bolts, we know on one hand there is a big risk, because there are a lot of hacker tools and a lot of known vulnerabilities that exist. On the other hand, we need to take that information and take it back to our own systems and say, well, we know what kind of things that the hackers might attack; we need to make sure that our systems are prepared to address those areas.

So there is a lot of progress, but we also have got to keep in mind that the risk, I think, is dramatically increasing. We are not dealing in a static risk environment. I think it is increasing; I think it will be a continuing challenge to make sure that those improvements keep pace, or in fact we need to outpace the increase in the risk to make progress, real progress.

Mr. HORN. What lessons can be learned from those agencies that are successfully improving their computer security?

Mr. DACEY. I think Mr. Lockhart addressed some of those issues in terms of security management.

We issued a guide in 1998 which really laid out a lot of the key issues. And GISRA was fundamentally based on some of the same principles, and your grades which you put up today are also based on security management concepts. And that is putting in place a key function responsible for computer security at a level in the agency that has the senior management's attention. That is a key aspect. Making sure you have got risk assessments, understanding what those risks are.

I know there are some governmentwide efforts now through NIST to develop standardized guidance for certification and accreditation that are now in draft and lay out three risk levels; and they intend to go further and define minimum controls for those risk levels, as well as techniques that can be used to assess them.

So we really have a structure that is starting to take place to assess the risks. I think those agencies that have gone ahead and done that, that are far advanced in the certification and accreditation process, have been able to demonstrate a better knowledge of their systems and in fact inventory their systems, which is something that is in the Federal Information Security Management Act, the fundamental process to make sure agencies have all their systems identified so they can begin that risk assessment process. And agencies like S SA, I think have done a reasonable job of trying to identify those systems and manage them. So that is important.

The second area is making sure you have the necessary controls. I think with some of the NIST efforts—that may go to help. I think it is a promising action that could help, because right now each agency is deciding on their own on what the controls they need to implement, and there isn't a constancy. And if we have that, as we talked about in testimony, I think, in July, there can be some constancy in training as well as tools developed to help people do what they need to do.

The third area is security awareness. I think a lot of agencies are now putting together programs to make sure that the employees are aware. Computer security is fine, but if someone can call up somebody in the agency and they willingly give up their password or use passwords that aren't very secure, that really endangers the whole system, not only that system, but anything it is connected to in a trusted environment. So I think that is another area where we have seen progress.

And the last area is really in the monitoring, and we are starting to see some agencies, such as Social Security, go outside to really have someone come in and help them test their systems to see if they are secure. I think that is a key component that has been long missing, but we are starting to see a lot of activity in that regard.

Also, as part of the certification and accreditation process, NIST is working on developing standards for accrediting entities that would do that.

I think one of the important elements, if we are going to proceed in this effort—and I think it is important—is to ensure some consistency in the types of testing of controls that are carried out, because right now there is a wide variation in the quality and extent of the procedures that may be used by the private sector. And I think bringing those to some consistency will be important.

So I think those are all aspects that, where agencies have done those kind of things and put responsibility in the CIO position, we are starting to see some fundamental changes. But again, those will take some time to come to fruition and for all the significant weaknesses we talked about to be identified.

Last, those significant weaknesses that I said in my testimony will likely increase, because I think we are still finding more of them, and as those get identified, hopefully those will get addressed as well, and we will get the numbers down.

Mr. HORN. In the help GAO and you have given us, to what degree are the agencies having very realistic, adequate contingency plans to recover their critical operations without a significant loss in their ability to conduct their mission?

Mr. DACEY. Based upon our review in the chart, we identified 20 agencies that had one or more significant weaknesses in contingency planning. And I think that is particularly important, because we were looking at report issued since September or after September of last year. And so that is a critical area. And I know a lot of agencies have been trying to address that, but again, to get back to fundamental issues: Do you know your systems? What they are? In some cases, we still struggle with that when we do our audits and go in, ask for inventories and structures of networks, we oftentimes don't get up-to-date pictures of what the agency has; and they need that.

Second, we have seen where there are plans, they may not be complete and assets properly prioritized, and probably one of the most important elements missing in many is really a comprehensive testing. Again, some agencies are doing that, but unless you comprehensively test this process—and I mean frequently; I don't know, there is no definite frequency, but with some degree of frequency—you don't know if it is going to work in case you have to employ it.

I know there are a lot of lessons learned based upon the effects of September 11 on the private sector, which we have had in prior testimonies before this committee. I think those are important lessons. Some of the more successful entities in the private sector had fairly extensive disaster recovery programs, as well as regular drills.

I do remember one of them, in fact, having practiced what happens if senior management, who makes the key decisions, isn't available to talk to. And, in fact, they practiced that, and that is what happened on September 11. They were busy evacuating lower Manhattan. The people who don't make day-to-day decisions had to make them, and they had prepared to do that by prior exercises.

So I think there are a lot of challenges still in that area, and in post-September 11 situations, particularly as Mr. Pethia pointed out, the increasing threats for intentional damage that might occur.

Mr. HORN. Are there any things that we have not brought up that would be useful in terms of getting a better type of a score in the last year or 2 more years, and there wouldn't be a lot of Fs all over that place? Let us see how many could be in Social Security, and that would help.

Mr. MEAD. I would like to see some tighter milestones. Having gone through the Y2K experience at Transportation, where we have a lot of operational systems like air traffic control or search and rescue, I think there is a very important value in having a date that everybody is marching toward. And the beauty of Y2K—it may be in hindsight, if I could use that word was that it had an unwaiverable date. It was certain to occur, and the agency heads and all the staffs knew that they were marching to get that done. And a serious computer security incident would get our attention, it might come too late.

Mr. HORN. Mr. Dacey.

Mr. DACEY. I would like to echo Mr. Mead's comments. I think one of the key areas that we have indicated in some of our prior reports and testimonies, both for Federal information and security and critical infrastructure protection, is the need to establish deadlines and goals.

I know one of the efforts that OMB has put forward as a result of last year's GISRA report is requiring all major agencies to undergo a project matrix review, which would identify significant assets of the agency and go about to identify interdependencies and come out with a plan to remedy those, any risks that they identified.

One of the challenges there though is, it has now taken a fair amount of time to get through that, and I don't know how many agencies have finished the first step. I know—Social Security has, I believe, already done that and is moving on in the second step.

But I think one of the challenges is, when does the government expect these actions to be—some of these key actions to be completed? And I think that is an important part of setting—again, a deadline helps to solidify what resources you need to get to that deadline. I think that could be beneficial.

Mr. HORN. I want to thank our witnesses today and the vice chairman, Mr. Lewis. And I am heartened by the administration's attention to this urgent problem. However, I am confident that the sustained pressure by the Office of Management and Budget, the General Accounting Office, and the Committee on Government Reform in the Congress, Federal agencies will continue to make strides to protect these vital systems.

We must solve this problem, and we must solve it quickly. The American people desire to know that the information they share with the Federal Government is protected. They must also be assured that the government services they rely on will not be interrupted.

I want to thank the subcommittee staff that has worked on this with a number of you. Bonnie Heald, the staff director, put your hand up; don't be shy around this place. Henry Wray, senior counsel; he is down working—he was very—working in terms of three bills we had the last night of this Congress, and they are about to go to be signed by the President. Counsel Dan Daly; Dan Costello, professional staff; the majority clerk, Chris Barkley; and staff assistant, Ursula Wojciechowski.

And then the detailee from the General Accounting Office has spent a lot of time on this. She is working here with my left hand and your right; and we are delighted with the General Accounting Office, and Elizabeth Johnston has done a wonderful job. I hope we can keep her longer, although I don't know; GAO might want her back, or at least put a chain on her. So she has done a great job.

And on the minority staff we have Michelle Ash, counsel, and Jean Gosa, the minority clerk. And they have done a wonderful job at every hearing I have done.

I thank the court reporters, Christina Smith and Desirae Jura. Thank you very much.

And, with that, we are adjourned.

[Whereupon, at 11:41 a.m., the subcommittee was adjourned.]

[Additional information submitted forthe hearing record follows:]

Third

REPORT CARD

On

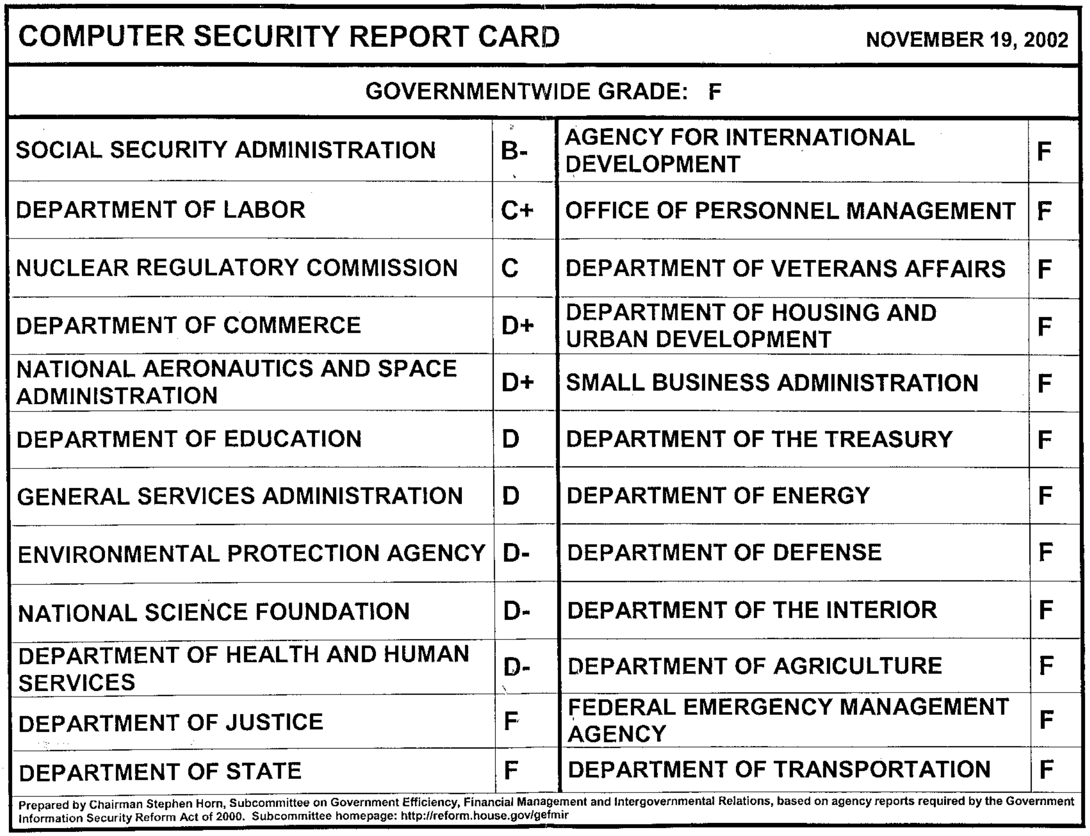
COMPUTER SECURITY

At

Federal Departments and Agencies

Overall Grade: F

November 19, 2002



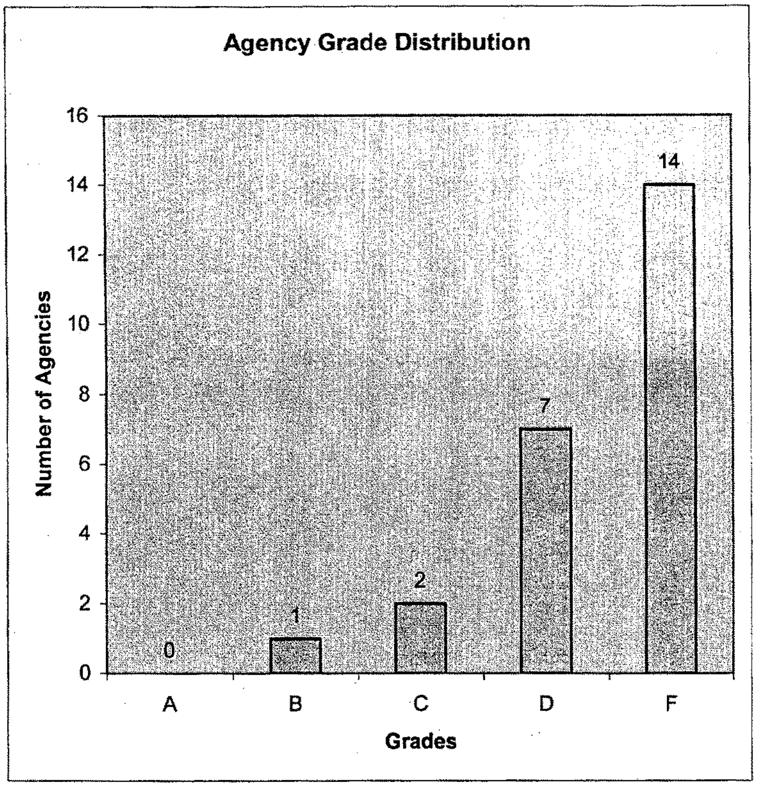
COMPUTER SECURITY REPORT CARD

NOVEMBER 19, 2002

GOVERNMENTWIDE GRADE: F

SOCIAL SECURITY ADMINISTRATION	B-	AGENCY FOR INTERNATIONAL DEVELOPMENT	F
DEPARTMENT OF LABOR	C+	OFFICE OF PERSONNEL MANAGEMENT	F
NUCLEAR REGULATORY COMMISSION	C	DEPARTMENT OF VETERANS AFFAIRS	F
DEPARTMENT OF COMMERCE	D+	DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT	F
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION	D+	SMALL BUSINESS ADMINISTRATION	F
DEPARTMENT OF EDUCATION	D	DEPARTMENT OF THE TREASURY	F
GENERAL SERVICES ADMINISTRATION	D	DEPARTMENT OF ENERGY	F
ENVIRONMENTAL PROTECTION AGENCY	D-	DEPARTMENT OF DEFENSE	F
NATIONAL SCIENCE FOUNDATION	D-	DEPARTMENT OF THE INTERIOR	F
DEPARTMENT OF HEALTH AND HUMAN SERVICES	D-	DEPARTMENT OF AGRICULTURE	F
DEPARTMENT OF JUSTICE	F	FEDERAL EMERGENCY MANAGEMENT AGENCY	F
DEPARTMENT OF STATE	F	DEPARTMENT OF TRANSPORTATION	F

Prepared by Chairman Stephen Horn, Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, based on agency reports required by the Government Information Security Reform Act of 2000. Subcommittee homepage: http://reform.house.gov/gefmir


Agency Grade Distribution
Number of Agencies
16
14
12
10
8
6
4
2
0
0
1
2
7
14
A
B
C
D
F
Grades

How Grades Were Assigned -- 2002 Computer Security Report Card

The subcommittee's computer security grades are based on information contained in agency reports to the Office of Management and Budget (OMB).

In October 2000, the President signed into law the Fiscal Year 2001 Defense Authorization Act (Public Law 106-398), which enacts a new subchapter on information security: Title X, Subtitle G, Government Information Security Reform (GISRA). This subchapter, known as the "Security Act," focuses on the program management, implementation, and evaluation of agency plans and procedures designed to protect the security of information technology systems that support Federal operations and assets. Among its provisions, the Act requires agency Chief Information Officers (CIOs) and Inspectors General (IGs) to evaluate their agency's computer security programs and report the results of those evaluations to the Office of Management and Budget (OMB) in September of each year, along with their budget submissions.

On July 2, 2002, the OMB provided revised reporting guidance on implementing the Security Act to agencies and agency inspectors general. Similar to guidance provided in 2001, the OMB instructed agencies and their inspectors general to submit executive summaries that include specific topics. These topics include the key elements of computer security management programs, as outlined in the Security Act. This year, however, the OMB also required that more specific performance metrics be used in the evaluations of agency performance.

In assigning grades, the subcommittee first assigned weighted point values to each OMB topic, with a perfect score totaling 100 points. As shown in the accompanying chart ("Analysis and Scoring Criteria,") point values were assigned for topics according to their importance to an agency's computer security program. The subcommittee's point values for each topic are consistent with the values assigned in determining last year's report card scores. Since most questions provide a range of possible responses, the number of points assigned to each response is proportional to the agencies' compliance with each topic. For example, when an agency summary found that agencies were 90 percent to 100 percent in compliance with the topic, they received the full weighted value. Agencies that had a 29 percent or lower compliance rate received zero (0) points. The subcommittee tallied agency scores based on an analysis of these responses.

Because this year's OMB guidance required agencies to respond to specific performance measures, these reports provided the subcommittee with a more reliable measurement of agency performance than in previous years.[*] Thus, the subcommittee did not factor the results of additional independent audits into the calculation of agency scores.

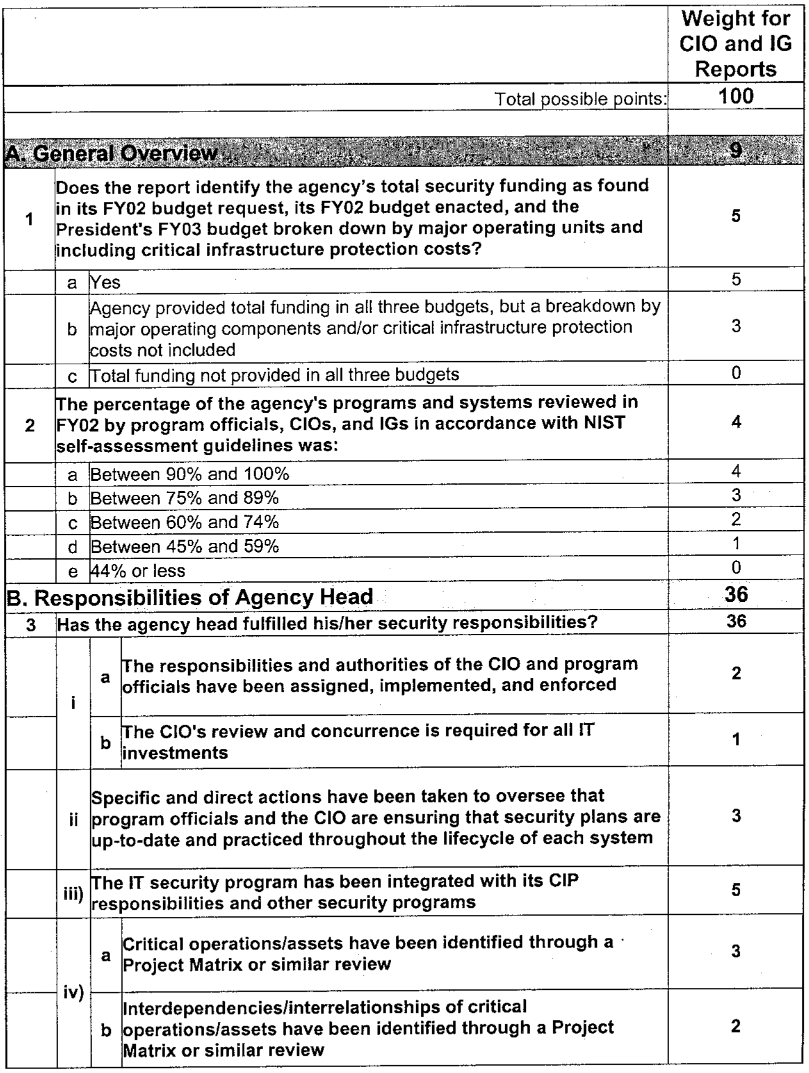
[*] In 2000, the first year that the subcommittee assigned agencies computer security grades, scores were primarily based on agencies' self-reporting in responses to a questionnaire developed by the subcommittee.

Letter grades for the 24 major departments and agencies were assigned as follows:

90 to 100 = A
80 to 89 = B
70 to 79 = C
60 to 69 = D
59 and lower = F

Scores that fall in the upper or lower portion of a grade range received either a "plus" (+) or "minus" (-), respectively. The Government-wide grade was determined by averaging the scores of all 24 agencies.

Analysis and Scoring Criteria for 2002 Report Card



				Weight for CIO and IG Reports
			Total possible points:	100
A. General Overview				**9**
1			**Does the report identify the agency's total security funding as found in its FY02 budget request, its FY02 budget enacted, and the President's FY03 budget broken down by major operating units and including critical infrastructure protection costs?**	5
	a		Yes	5
	b		Agency provided total funding in all three budgets, but a breakdown by major operating components and/or critical infrastructure protection costs not included	3
	c		Total funding not provided in all three budgets	0
2			**The percentage of the agency's programs and systems reviewed in FY02 by program officials, CIOs, and IGs in accordance with NIST self-assessment guidelines was:**	4
	a		Between 90% and 100%	4
	b		Between 75% and 89%	3
	c		Between 60% and 74%	2
	d		Between 45% and 59%	1
	e		44% or less	0
B. Responsibilities of Agency Head				**36**
3			**Has the agency head fulfilled his/her security responsibilities?**	36
	i	a	**The responsibilities and authorities of the CIO and program officials have been assigned, implemented, and enforced**	2
		b	**The CIO's review and concurrence is required for all IT investments**	1
	ii		**Specific and direct actions have been taken to oversee that program officials and the CIO are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system**	3
	iii)		**The IT security program has been integrated with its CIP responsibilities and other security programs**	5
	iv)	a	**Critical operations/assets have been identified through a Project Matrix or similar review**	3
		b	**Interdependencies/interrelationships of critical operations/assets have been identified through a Project Matrix or similar review**	2

	v)	Subsequent to the Project Matrix (or similar review), critical operations/assets have been secured		5
	vi)	He/she has ensured that all agency components have documented procedures for reporting security incidents and sharing common vulnerabilities and incidents are reported to FedCIRC or law enforcement in accordance with federal guidance		12
	vii)	The agency has oversight procedures to verify that patches are tested and installed in a timely manner		3
C. Responsibilities of Agency Program Officials				17
4	Have program officials fulfilled their security responsibilities?			17
	i)	The percentage of systems that have been assessed and have a level of risk assigned is:		2
		a	Between 90% and 100%	2
		b	Between 75% and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45% and 59%	0.5
		e	44%or less	0
	ii)	The percentage of systems that have an up-to-date security plan is:		2
		a	Between 90% and 100%	2
		b	Between 75% and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45% and 59%	0.5
		e	44% or less	0
	iii)	The percentage of systems that have been authorized for processing following certification and accreditation is:		2
		a	Between 90%and 100%	2
		b	Between 75% and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45% and 59%	0.5
		e	44% or less	0
	iv)	The percentage of systems that have the costs of their security controls integrated into the life cycle of the system is:		2
		a	Between 90% and 100%	2
		b	Between 75% and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45 and 59%	0.5
		e	44% or less	0
	v)	The percentage of systems whose security controls have been tested and evaluated in the last year is:		2
		a	Between 90% and 100%	2
		b	Between 755 and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45% and 59%	0.5
		e	44% or less	0

	vi)	The percentage of systems that have a contingency plan that has been tested in the past year is:		**2**
		a	Between 90% and 100%	2
		b	Between 75% and 89%	1.5
		c	Between 60% and 74%	1
		d	Between 45% and 59%	0.5
		e	44% or less	0
	vii)	For operations and assets under their control, the percentage of contractor provided services or services provided by another agency for their program and systems that have been reviewed is:		**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1
		f	29% or less	0
		g	No contractor provided services or services provided by another agency.	5
D. Responsibilities of Agency Chief Information Officer				**38**
5	**Has the CIO fulfilled his/her security responsibilities?**			**38**
	i)	The percentage of agency components and field activities that have received security reviews (other than GAO or IG audits) is:		**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1
		f	29% or less	0
	ii)	The percentage of agency employees (including contractors) that received security training informing them of their jobs' information security risks and their responsibilities in complying with agency information security policies and procedures is:		**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1
		f	29% or less	0
	iii)	The percentage of employees with significant security responsibilities that received specialized security training is:		**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1

		f	29% or less	0
	iv)		**The agency provided the total training costs**	**5**
	v)		**Agency corrective action plans address all identified significant weaknesses**	**6**
	vi)		**The CIO has appointed a senior agency information security official**	**5**
	vii)		**For operations and assets under his/her control, the percentage of contractor provided services or services provided by another agency that have been reviewed is:**	**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1
		f	29% or less	0
		g	No contractor provided services or services provided by another agency.	5
	viii)		**The percentage of capital asset plans that include the requisite security information and costs and have been independently validated by the CIO/other appropriate official prior to submittal to OMB is:**	**5**
		a	Between 90% and 100%	5
		b	Between 75% and 89%	4
		c	Between 60% and 74%	3
		d	Between 45% and 59%	2
		e	Between 30% and 44%	1
		f	29% or less	0
	ix)		**Security costs for all agency systems were reported on the exhibit 53**	**3**

Computer Security Grades
2000-2002

Agency	2000 Score	2000 Grade	2001 Score	2001 Grade	2002 Score	2002 Grade
Agriculture	56	**F**	31	**F**	36	**F**
AID	72	**C-**	22	**F**	52	**F**
Commerce	72	**C-**	51	**F**	68	**D+**
DOD	69	**D+**	40	**F**	38	**F**
Education	75	**C**	33	**F**	66	**D**
Energy	INC*	**INC***	51	**F**	41	**F**
EPA	64	**D**	69	**D+**	63	**D-**
FEMA	INC*	**INC***	65	**D**	33	**F**
GSA	61	**D-**	66	**D**	64	**D**
HHS	58	**F**	43	**F**	61	**D-**
HUD	73	**C-**	66	**D**	48	**F**
Interior	17	**F**	48	**F**	37	**F**
Justice	52	**F**	50	**F**	56	**F**
Labor	38	**F**	56	**F**	79	**C+**
NASA	60	**D-**	70	**C-**	68	**D+**
NRC	INC*	**INC***	34	**F**	74	**C**
NSF	80	**B-**	87	**B+**	63	**D-**
OPM	59	**F**	39	**F**	52	**F**
SBA	55	**F**	48	**F**	48	**F**
SSA	86	**B**	79	**C+**	82	**B-**
State	75	**C**	69	**D+**	54	**F**
Transportation	INC*	**INC***	48	**F**	28	**F**
Treasury	65	**D**	54	**F**	48	**F**
VA	65	**D**	44	**F**	50	**F**
Governmentwide Average	**INC**	**D-**	**53**	**F**	**55**	**F**

Agency 2000-2002 scores and grades are based on reports on the previous years' security reviews and evaluations.

*Agencies with three or more general control categories that had not been audited were not assigned a grade. Instead they were given "INC" for incomplete. The Government-wide grade was determined by averaging the final scores of all that received grades; agencies with "incomplete" were not included in calculating this average.