PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE: HOW SECURE ARE GOVERNMENT COMPUTER SYSTEMS?

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

APRIL 5, 2001

Serial No. 107–13

Printed for the use of the Committee on Energy and Commerce

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

U.S. GOVERNMENT PRINTING OFFICE

72–834CC WASHINGTON : 2001

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 ENERGY AND COMMERCE

W.J. "BILLY" TAUZIN, Louisiana, *Chairman*

MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
TOM DAVIS, Virginia
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
CHARLES F. BASS, New Hampshire
JOSEPH R. PITTS, Pennsylvania
MARY BONO, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
CHRISTOPHER JOHN, Louisiana
JANE HARMAN, California

DAVID V. MARVENTANO, *Staff Director*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

JAMES C. GREENWOOD, Pennsylvania, *Chairman*

MICHAEL BILIRAKIS, Florida
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
ED WHITFIELD, Kentucky
Vice Chairman
CHARLES F. BASS, New Hampshire
W.J. "BILLY" TAUZIN, Louisiana
(Ex Officio)

PETER DEUTSCH, Florida
BART STUPAK, Michigan
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
CHRISTOPHER JOHN, Louisiana
BOBBY L. RUSH, Illinois
JOHN D. DINGELL, Michigan,
(Ex Officio)

(II)

CONTENTS

Page

Testimony of:

Dacey, Robert F., Director, Information Security Issues, U.S. General Accounting Office 53

Dick, Ronald L., Director, National Infrastructure Protection Center 30

McDonald, Sallie, Assistant Commissioner, Office of Information Assurance and Critical Infrastructure, U.S. General Services Administration 26

Noonan, Tom, President and CEO, Internet Security Systems, Inc 39

Podonsky, Glenn S., Director, Office of Independent Oversight and Performance Assurance, accompanied by Jason Bellone, former member of the Computer Analysis Response Team, Federal Bureau of Investigation; Karen Matthews, formerly with Computer Forensics Laboratory, U.S. Department of Defense; Brent Huston, author of book on hackproofing; and Brad Peterson, Director, Office of Cyber Security and Special Reviews, U.S. Department of Energy 13

Tritak, John S., Director, Critical Infrastructure Assurance Office, U.S. Department of Commerce 65

Material submitted for the record by:

Kemper, Jason, III, Vice President, Government Affairs, Cryptek, letter dated April 5, 2001, enclosing testimony for the record 76

PROTECTING AMERICA'S CRITICAL INFRASTRUCTURE: HOW SECURE ARE GOVERNMENT COMPUTER SYSTEMS?

THURSDAY, APRIL 5, 2001

HOUSE OF REPRESENTATIVES,
COMMITTEE ON ENERGY AND COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:40 a.m., in room 2322, Rayburn House Office Building, Hon. James C. Greenwood (chairman) presiding.

Members present: Representatives Greenwood, Tauzin, (ex officio), Strickland, and DeGette.

Also present: Representatives Norwood and Davis.

Staff present: Tom DiLenge, majority counsel; Amit Sachdev, majority counsel; Peter Kielty, legislative clerk; and Edith Holleman, minority counsel.

Mr. GREENWOOD. This hearing of the Oversight and Investigations Subcommittee will come to order. The Chair recognizes himself for 5 minutes for the purpose of an opening statement.

Today, the subcommittee holds a hearing to assess the security of government computer systems. In particular, we will assess how well or how poorly they are protecting our most critical cyberinfrastructures and operations from the threat of disgruntled insiders, hackers, criminals, terrorists, and rogue nation-states. Over the past 2 years this committee has conducted extensive oversight of computer security at particular government agencies, most notably EPA, the Department of Energy, and to a lesser extent, FDA and the Department of Commerce. Our reviews consistently have found poor computer security planning and management and a general lack of compliance with existing requirements of law and policy.

We also found that, with few exceptions, the agencies were not testing their own systems to determine whether their security plans and policies were as effective in practice as they looked on paper. And we found that whenever real testing of agency systems was conducted numerous significant and easily exploitable vulnerabilities were almost always discovered.

In response, Congress passed a law last October that reiterated computer security requirements contained in prior Federal laws and OMB directives mandating that agencies develop security plans for their systems and conduct periodic risk assessments and tests of those systems. But it also imposed a new requirement, that

agency inspectors general conduct an independent test of an appropriate subset of agency systems each year.

One month ago, in order to set a benchmark for measuring agency progress under this new law, I wrote to 15 Federal departments, agencies, and commissions within this committee's jurisdiction to inquire about their compliance with computer security directives and their plans to implement the new law. While a few of the agencies are still in the process of producing documentation for us, it is fair to say that, at this point, we are not surprised or pleased by what we are finding.

In particular, very few of the responding agencies have had any true penetration tests of their computer systems conducted and many of these were very limited in nature and scope, conducted as part of financial system audits. A few other agencies have conducted automated scans of their network to search for vulnerabilities in their configurations or operating systems which, while worthwhile, do not reveal the real degree of potential exploits of their systems. And several other agencies reported no scans or penetration tests whatsoever.

Also, not surprising, the tests and scans that have been done continue to reveal real computer security problems at these agencies:

A recent internal scan conducted by a Commerce Department bureau found more than 5,000 security "holes," or known vulnerabilities, in its networks and systems; and that of 1,200 hosts or workstations scanned, fully 30 percent suffered from category "red" vulnerabilities, which is the most severe rating because of the potential to compromise an entire account.

An internal test of a Medicare contractor 2 years ago found, unbelievably, that the network system administrator's account—let me repeat that, the network system administrator's account—could be easily compromised because his password was the same as his user name.

A recent internal test of a critical HHS operating division, using freely available password cracking software, resulted in 60 percent of passwords being cracked in under 10 minutes.

Unfortunately, these findings are not the exception. They are just some of the many examples of poor computer security we are finding during the course of our review. Consistent with the broad swath of GAO and inspector general computer security audits across the Federal Government over the past 4 or 5 years.

I point these out not to embarrass particular agencies—actually, they should be commended for testing their systems to find these problems in the first place—but rather to emphasize the need for the Federal Government to begin taking cybersecurity much more seriously than we have been. They also clearly demonstrate the need to increase our level of testing so that problems can like these can be found and corrected before real damage is done.

Why is this so important? Because as we will see and hear today, the threats and attacks on government systems are increasing and the technology used to perpetrate such attack is becoming both more sophisticated and more generally available. An expert team from the Department of Energy will demonstrate this morning how such attacks are conducted, using freely available software tools

found on the Internet, and they will show us the results from some recent real-world testing the team conducted at several DOE sites.

For its part, GSA, which tracks overall security incidents at Federal civilian agencies, will testify today that in the year 2000 alone 32 agencies reported 155 known "root" compromises of their computer systems, the most serious type of incident tracked because the unauthorized user was able to gain complete control of the server or system compromised.

GSA also will testify that there were hundreds of incidents of network reconnaissance reported by 18 different civilian agencies last year, mostly from foreign sources and targeting our scientific facilities. And these are only the incidents we know about. GSA estimates that only 20 percent of all known incidents are reported by the agencies and there likely are thousands more that go undetected by the agencies themselves.

GSA and other experts in this field also estimate that nearly all of the incidents reported on both government and private systems could have been prevented had the system administrators fixed well-known vulnerabilities with existing patches or configuration changes.

While no network can ever be 100 percent secure from the most sophisticated and novel attacks, it should not be an unreasonable expectation that our sensitive systems would be secure from commonly known vulnerabilities.

Finally, as the title of this hearing suggests, we also will focus today on the related issue of critical cyberinfrastructure protection, that is, the protection of those Federal cybersystems that are truly critical to the Nation's security for the public's health and welfare. Not all computer systems are created equal, nor do they deserve the same level of security attention.

The Clinton administration realized the need to focus the attention on threats posed to our most critical cybersystems by terrorists or others intent on doing the Nation harm. Accordingly, in May 1998, the President issued a directive mandating the Federal agencies identify their critical assets, assess the vulnerabilities of those assets, and then implement plans to fix the vulnerabilities by May 2003. However, several recent reports confirm what the committee's own review has found that, 3 years later, most agencies are still in the process of identifying their critical assets and virtually none have made significant progress in assessing and mitigating vulnerabilities in those systems or the private sector resources on which these Federal systems so often rely. Given this state of affairs, it appears that we will not meet this deadline unless we dramatically increase our focus on this problem in the very near term.

Clearly, we need to do better both with respect to critical cybersystems and to overall computer security throughout the Federal Government. I hope that today's hearing will be the first in a series on these important and related topics, that we can work together on both sides of the aisle and with this new administration to improve the security of our Nation and the sensitive data held by our Federal Government.

The Chair recognizes Mr. Strickland for an opening statement.

Mr. STRICKLAND. Mr. Chairman, thank you for holding this hearing on this very important question.

As one of our witnesses will testify today, the existence of the Internet ties together a vast array of computer systems and networks. For communications, commerce, and the democratic exchange of ideas, there are enormous benefits from this full and open access; but like any technology that is new, or relatively new, it has a serious downside. By tying these networks together, the Internet makes them all vulnerable to hacking by creative teenagers and others with more nefarious purposes such as fraud, identity theft, extortion, disruptions of commercial service, and terrorist attacks.

One system can be used as a platform to attack other systems. Without appropriate safeguards, any system can be hit, whether it is essential to our defense and economy or it is a site that sells goods in an electronic auction; and it appears that the attempts to penetrate both government and private systems are increasing. We must recognize that no system will ever be completely secure, but the question is whether the Federal response to safeguard their critical assets is adequate and whether it has the resources to respond fully.

A great deal was done by the previous administration to begin to address this enormous task. President Clinton established a Commission on Critical Infrastructure Protection in July 1996 to look at the scope and the nature of vulnerabilities and threats to the Nation's critical infrastructures and to recommend a comprehensive national policy and implementation plan for protecting them, whether public or private.

The result was the commission's 1997 report, which found no immediate crisis threatening the infrastructure, but did find that threat to and the vulnerability of the critical infrastructure existed. President Clinton responded by issuing Presidential Decision Directive 63 in May 1998, which ordered the Federal agencies to identify their critical infrastructures, take steps to protect them and work cooperatively with private companies which control most of the infrastructure, to secure those systems also. The target date for completion was May of 2003.

Presidential Directive 63 listed the areas in which the infrastructure should be protected, and established the position of National Coordinator for Security and for Structural Protection and Counterterrorism in the National Security Council. It set up the critical Infrastructure Assurance Office at the Commerce Department to support the national coordinator and the agencies and gave the Federal Bureau of Investigation the explicit authority to expand its existing cybercrimes unit into the National Infrastructure Protection Center.

Prior to this Presidential directive, President Clinton had already established a Federal computer intrusion response capability, which is housed at the General Services Administration. A national plan for information systems protection, the first in the world by a national government, was issued in January of 2000. And just before he left office, President Clinton nominated 18 members of the National Infrastructure Assurance Council, which is to report on the actions of private and public bodies to protect their critical infrastructures.

Three industry sectors also have established information sharing and analysis centers.

How far along are the agencies in implementing the Presidential directive? Certainly they are ahead of where they were 5 years ago when cybersecurity was given little, if any, attention, but they are not far enough along and they remain vulnerable. As we will hear from the Commerce Department witnesses, most agencies still have to finish identifying their critical infrastructure assets. They will not meet the 2003 deadline without significant additional resources.

Furthermore, no one know if the structure established by the previous administration to enforce Presidential Directive 63 will be continued by the new administration. The old structure was not perfect, and there are numerous overlapping and conflicting responsibilities resulting from the differing directives in PDD-63 and various other laws. But we must request that the Bush administration tread lightly and consider whether a completely new structure will delay even longer this very important task.

A question for the Congress to address is whether the agencies are getting the money they need to get the job done. This body has not been particularly responsive to appropriations for computer security, as evidenced by its rejection of most of the requests last year for beefing up the Energy Department security, its rejection of the $50 million request for an Institute for Information Infrastructure Protection, and an almost 50 percent reduction in GSA's request for funding for their needs.

One other concern I must mention, however, is privacy. GSA has published a very disturbing newsletter that tells agencies to get around Congress' and the public's concerns about being tracked by Federal agencies by contracting out the service and calling it something else. I have attached that document to my testimony and would like it placed in the record.

Mr. Chairman, these are all issues that I hope this subcommittee will address in the next several months. I may have additional documents to place in the record and would request that the record be held open for that purpose.

Thank you, Mr. Chairman.

Mr. GREENWOOD. The Chair thanks the gentleman. Without objection his attachment will be entered into the record.

[The prepared statement of Hon. Ted Strickland follows:]

PREPARED STATEMENT OF HON. TED STRICKLAND, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF OHIO

Mr. Chairman, thank you for holding this hearing on this very important question. The existence of the Internet ties together a vast array of computer systems and networks. For communications, commerce and the democratic exchange of ideas, there are enormous benefits from full and open access to these systems. But, like any technological advance, it also has a serious downside. By tying these networks together, the Internet makes them all vulnerable to hacking by creative teen-agers and others with more nefarious purposes such as: fraud; identity theft; extortion; disruptions of commercial service; and terrorist attacks. One system can be used as a platform to attack other systems. Without appropriate safeguards, any system can be hit, whether it is essential to our defense and economy, or it is a site that sells goods in an electronic auction. And it appears that the attempts to penetrate both government and private systems are increasing.

We must recognize that no system will ever be completely secure, but the question is whether the federal government's response to safeguard its critical assets is ade-

quate, and whether it has the resources to fully respond. A great deal was done by the previous administration to begin to address this enormous task. President Clinton established a Commission on Critical Infrastructure Protection in July of 1996 to look at the scope and nature of vulnerabilities and threats to the nation's critical infrastructures and recommend a comprehensive national policy and implementation plan for protecting them, whether public and private. The Commission's 1997 report found no immediate crisis threatening the infrastructure, but did find that the threat to and vulnerability of the critical infrastructure existed. President Clinton responded by issuing Presidential Decision Directive 63 in May of 1998. It ordered federal agencies to identify their critical infrastructures, take steps to protect them and work cooperatively with private companies—which control most of the infrastructure—to secure those systems also. The target date for completion was May of 2003.

PDD 63 listed the areas in which the infrastructures should be protected, and established the position of national coordinator for security, infrastructure protection and counter-terrorism in the National Security Council. It set up the Critical Infrastructure Assurance Office at the Commerce Department to support the national coordinator and the agencies and gave the Federal Bureau of Investigation the explicit authority to expand its existing cyber crimes unit into the National Infrastructure Protection Center (NIPC). Prior to PDD 63, President Clinton had already established a Federal Computer Intrusion Response Capability, or "Fed CIRC", which is housed at the General Services Administration. A national plan for information systems protection—the first in the world by a national government—was issued in January of 2000. And just before he left office, President Clinton nominated 18 members of the National Infrastructure Assurance Council, which is to report on the actions of private and public bodies to protect their critical infrastructures. Three industry sectors also have established Information Sharing and Analysis Centers or ISACs.

How far along are the agencies in implementing PDD 63? Certainly, they are ahead of where they were five years ago when cyber security was given little, if any, attention. But they are not far enough along, and they remain vulnerable. As we will hear from the Commerce Department witnesses, most agencies still have to finish identifying their critical infrastructure assets. They will not meet the 2003 deadline without significant additional resources.

Furthermore, no one knows if the structure established by the previous administration to enforce PDD-63 will be continued in the new administration. The old structure was not perfect, and there are numerous overlapping and conflicting responsibilities resulting from the differing directives in PDD-63 and various laws. But the Bush Administration should tread lightly and consider whether a completely new structure will delay even longer this very important task.

A question for the Congress to address is whether the agencies are getting the money they need to get the job done. This body has not been particularly responsive to appropriations for computer security as evidenced by its rejection of most of the request last year for beefing up the Energy Department's security; its rejection of NIST's $50 million request for an Institute for Information Infrastructure Protection; and an almost 50 percent reduction of GSA's request for funding for Fed CIRC.

One other concern that I must mention, however, is privacy. GSA has published a very disturbing newsletter that tells agencies to get around Congress' and the public's concerns about being tracked on the Internet by federal agencies by contracting out the surveillance to private contractors and calling it "Management Security Services." I have attached that document to my testimony and would like it placed into the record.

Mr. Chairman, these are all issues that I hope this Subcommittee will address in the next several months. I may have additional documents to place in the record and would like to request that the record to be held open for that purpose.

Mr. NORWOOD. Mr. Chairman, I ask unanimous consent that I may make a brief opening statement.

Mr. GREENWOOD. Mr. Norwood, while an esteemed member of the Energy and Commerce Committee, does not have the honor of serving on this subcommittee. But we have the honor of his presence, and without objection, we will ask that he be offered time for an opening statement.

Mr. NORWOOD. Thank you very much, Mr. Chairman.

I am here for two or three reasons this morning, one of which is to thank you and to congratulate you and to tell you how pleased

I am that you are taking the Commerce Committee in this direction in terms of the security for our Nation. I thank you for that, and I hope, too, you will have many other hearings.

To give you some indication of how important I think this subject is, about right now we are teeing off the first tee in the Augusta National this morning, my home district, and I promise you I would have loved to have been there, but I view this as a little more important.

The other reason I wanted to come this morning is because I am very pleased with the witnesses and especially that you have the President and CEO of Internet Security Systems here as a big player in all of this. ISS has been recognized as the worldwide leader, Mr. Chairman, in the intrusion detection and vulnerability assessment market. In addition, ISS has become the world's largest provider of managed security service, and they deliver a 24-7 security monitoring and management, just sort of something we might be interested in. And I guess I am just real tickled that a Georgia company has played such a leading role in this extremely important area.

We have indications that this area of computer security is growing very, very rapidly. For example, ISS has been named the fifth fastest growing technology company in North America and, listen to this, this is based on a 5-year revenue growth of 45,000 percent. There is some indication in that number that tells us all how important this is and must be.

This achievement demonstrates to me that this is a large emerging area that will impact today's Internet economy.

Now, the government has taken strides—I don't know whether to say great or good—but at least strides in the past few years. However, as you know, much more is needed. Funding must be increased by a substantial amount if we take this seriously. As industry has considered resources and expertise, a continued partnership with industry on this subject is going to be very critical; and it is my understanding that ISS has played a leadership role in working and partnering with the government on security issue s. And with any private company you do that with some risk, but I think and hope this relationship will continue, not just because it is good for a Georgia company, but because it is so very needed for the national security of this Nation. And with that, Mr. Chairman, I will submit the rest for the record and thank you for your courtesy and kindness this morning.

Mr. GREENWOOD. The Chair thanks the gentleman. Without objection, the rest of his testimony, as well as the testimony of all other members who may submit them, will be entered into the record. Also a member of the committee, but not a member of the Oversight and Investigation Subcommittee, is Mr. Davis of Virginia, and we are happy to have him here as well.

Mr. DAVIS. Thank you very much. Let me—Mr. Chairman, I ask unanimous consent that I be able to make some comments.

Mr. GREENWOOD. Without objection.

Mr. DAVIS. Thanks for allowing me to participate in this hearing today. I want to compliment you and your staff on the diligent work on this pressing issue. It is vitally important that we in Congress recognize and understand the complexities we face in pur-

suing our Nation's critical infrastructure, the systematic activities that are essential to the minimum operation of our economy and government.

Although 95 percent of our critical infrastructure is owned and operated by the private sector as your Nation's front line, the Federal Government plays an essential role in sharing information about cyberthreats against our assets. But the evidence demonstrates that the Federal Government is dangerously behind the curve in getting its own house in order. Simply put, we are losing time. Since 1997, GAO has listed information security as a governmentwide high-risk area and has conducted numerous reviews which have continuously sounded the alarm about widespread weakness and vulnerabilities in the Federal Government's information systems.

During March of last year, as part of a review requested by the Subcommittee on Government Management Information and Technology, of which I was a member, GAO has found that 22 of the largest Federal agencies were providing inadequate protection to critical Federal operations and assets from computer-based attacks. They were able to identify systemic weaknesses in the information security practice of the Department of Defense, the National Aeronautics and Space Administration, the Department of State, and the Department of Veterans Affairs; and then, as many of you know, in September of 2000, the subcommittee gave the Federal Government an overall D-minus on its computer security practices report card.

Just as the Romans built the greatest network of roads at the height of the Roman Empire and the barbarians used these same networks to destroy the Romans, so we may face the same vulnerabilities with the advances we have made in technology and the interconnectivity of our networks. There is no doubt that nations are in the process of developing tools to penetrate and cripple these networks.

At the same time, the outside world is but one source of the threat to government information systems. Much of the threat comes from within the government. A key challenge to making the Federal Government more secure lies in the mindSet of many Federal agencies vis-a-vis the importance of information security to their operations and assets.

For many, implementing best practices for controlling and protecting information resources is just a low priority. The question before us then is, what do we do about it? What steps should Congress take to change the direction and reduce the vulnerability of Federal operations and assets?

As one who has studied the issue for over a year, I come to the conclusion there are two necessary components to achieving the goal. First, I strongly believe there is a dire need for a strong central leader who can coordinate implementation of information security best practices across government. Currently, these responsibilities are shared by several Federal agencies, some of whom are before us today, which make the coordination and uniformity of information security practices a formidable obstacle.

The government information security community needs an advocate who can ensure that information security becomes an inte-

grated component of information systems. Let me say I agree with those who assert that funding for implementing information security measures is inadequate. I submit that having a Federal CIO with this responsibility, as I put forth in legislation, who can champion the agency's security needs, would be an effective voice in this respect.

Second, we need to encourage information sharing between the private sector and government. As many of our witnesses would likely agree, the ownership dynamic of our Nation's critical assets makes crucial the development of thriving public-private partnerships for this purpose, but with the current Federal computer systems it is, in my mind, entirely reasonable that many in the private sector are wary of entering into these partnerships. At the same time, current law is retarding the implementation of the National Infrastructure Assurance Plan. It is for this reason we introduced legislation last year that gives critical infrastructure industries the assurances they need to confidently share information with the Federal Government.

Our measure would provide a limited FOIA exemption, civil litigation protection for shared information, and an antitrust exemption for information shared within an information sharing and analysis. These three protections were cited by the past administration as necessary legislative remedies. This legislation would enable the ISACs to move forward without fear from industry, so that government and industry could enjoy the mutually cooperative partnership called for in the PDD-63.

I ask unanimous consent the rest of my statement be put in the record, and I appreciate the opportunity to be here today.

Mr. GREENWOOD. Without objection, the gentleman's statement in its entirety will be placed in the record.

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

PREPARED STATEMENT OF HON. TOM DAVIS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA

Mr. Chairman, thank you very much for allowing me to participate today in this hearing. I want to compliment you and your staff for your diligent work on this pressing issue.

It is vitally important that we in Congress recognize and understand the complexities we face in pursuing the protection of our nation's critical infrastructure—those systemic activities that are essential to the minimum operations of our economy and government. Although 95% of our critical infrastructure is owned and operated by the private sector, as our nation's front line, the Federal Government plays an essential role in sharing information about cyber threats against our assets.

But the evidence demonstrates that the Federal Government is dangerously behind the curve in getting its house in order. Simply put, we are losing time. Since 1997, GAO has listed information security as a governmentwide high risk area and has conducted numerous reviews which have continuously sounded the alarm about widespread weaknesses and vulnerabilities in the Federal Government's information systems. During March of last year, as part of a review requested by the Subcommittee on Government Management, Information, and Technology, of which I was a Member, GAO found that 22 of the largest federal agencies were providing inadequate protection for critical federal operations and assets from computer-based attacks. They were able to identify systemic weaknesses in the information security practices of the Department of Defense, the National Aeronautics and Space Administration, the Department of State, and the Department of Veterans Affairs. And then as many of you know, in September 2000, the Subcommittee gave the Federal Government an overall D- on its computer security practices report card.

Just as the Romans built the greatest network of roads at the height of the Roman Empire and the Barbarians later used this same network to destroy the Ro-

mans, so may we face the same vulnerabilities with the advances we have made in technology and the interconnectivity of our networks. There is no doubt that nations are in the process of developing tools to penetrate and cripple these networks.

At the same time, the outside world is but one source of the threat to government information systems. Much of the threat comes from within the government. A key challenge to making the Federal Government more secure lies in the mind set of many federal agencies vis-a-vis the importance of information security to their operations and assets. For many, implementing best practices for controlling and protecting information resources is a low priority.

The question before us then is what do we do about it? What steps should Congress take to change the direction and reduce the vulnerability of federal operations and assets?

As one who has studied these issues for over a year now, I have come to the conclusion that there are two necessary components to achieving this goal. First, I strongly believe that there is dire need for a strong central leader who can coordinate the implementation of information security best practices across government. Currently, these responsibilities are shared by several federal agencies (some of whom are before us today), which makes the coordination and uniformity of information security practices a formidable obstacle. The government information security community needs an advocate who can ensure that information security becomes an integrated component of information systems. Let me also say that I agree with those who assert that funding for implementing information security measures is inadequate, and I submit that having a Federal CIO with this responsibility as I have put forth in legislation, who can champion the agencies' security needs, would be an effective voice in this respect.

Second, we need to encourage information sharing between the private sector and government. As many of our witnesses would likely agree, the ownership dynamic of our nation's critical assets makes crucial the development of thriving public/private partnerships for this purpose. Yet with the current state of Federal computer systems, it is in my mind entirely reasonable that many in the private sector are wary of entering into those partnerships. At the same time, current law is retarding the implementation of the National Infrastructure Assurance Plan. It is for this reason that I introduced legislation last year that gives critical infrastructure industries the assurances they need in order to confidently share information with the Federal Government. My measure would provide a limited FOIA exemption, civil litigation protection for shared information, and an antitrust exemption for information shared within an Information Sharing and Analysis (ISAC). These three protections were cited by the past Administration as necessary legislative remedies in Version 1.0 of the National Plan for Information Systems Protection and PDD-63. This legislation would enable the ISACs to move forward without fear from industry so that government and industry may enjoy the mutually cooperative partnership called for in PDD-63.

As Chairman of the House Government Reform Subcommittee on Technology and Procurement Policy, I will be continuing to explore this matter, along with Chairman Steve Horn of the Government Efficiency, Financial Management, and Intergovernmental Affairs Subcommittee. I am grateful that you, Mr. Chairman, have also taken an active approach to addressing this problem today, and I look forward to working with you to make the Federal Government a model for risk management and the protection of information systems. As well, I am pleased to have the opportunity to hear the testimony of our distinguished panelists and appreciate their being here. I want to particularly welcome here today, Mr. Tom Noonan, the President and CEO of Internet Security Systems, which is headquartered in Atlanta but has an important presence in my district. I look forward to hearing from all of you.

Mr. GREENWOOD. The Chair recognizes the chairman of the full committee, the gentleman from Louisiana, Mr. Tauzin, for an opening statement.

Chairman TAUZIN. Thank you, Mr. Chairman, for holding this important hearing on the inadequacy of the Federal efforts to protect our Nation's critical cyberinfrastructure and the vast amount of sensitive data that is stored on Federal computer systems.

I really don't think that many people realize the extent to which the Federal civilian agencies collect and store so much sensitive information, whether it is medical, financial or other personal information on American citizens, confidential, proprietary data from

America's corporations, cutting-edge scientific research, or whether it is export controlled information or even sensitive law enforcement information. There are tons of it that is subject to hacking and to compromise.

We learned, for example, in the GAO report that even the IRS had allowed a cookie on its Web site. Nor do most people realize the extent to which we as a Nation have become so independent on these computer systems to assure our national economic security, and I think it would come as quite a surprise for most Americans to learn which these Federal agencies are the target of attacks by foreign and domestic sources bent upon espionage and other very malicious actions.

Faced with this kind of serious challenge, the Federal Government has not performed well. This committee's oversight continues to reveal troubling computer security deficiencies across the Federal Government, deficiencies that place critical services and sensitive data at significant risk of compromise. Here, the connection between the security and the privacy of American citizens cannot be ignored.

A recent inspector general's audit of the Health Care Financing Administration and several of its Medicare contractors, which the committee is releasing publicly today, found numerous system control weaknesses that permitted unauthorized access to sensitive beneficiary information. This is sensitive health care information about Americans that we discovered could be easily compromised in the Federal HCFA systems; and while we don't know today whether the information was in fact compromised, we intend to find out whether that has in fact happened. And I can assure you, in a private conversation I had with Secretary Thompson yesterday, he intends to see what is going on at HCFA in this critical area and he intends to get it fixed before this is an issue of enormous importance to Americans and one that this committee, I hope, Mr. Chairman, will continue to take a very close and diligent look at.

The Clinton administration talked a great deal about cybersecurity and critical infrastructure protection over the past several years, holding Presidential summits and issuing Presidential directives. The administration, for example, said the Federal Government would serve as a model for good security practice for the private sector, which controls much of the Nation's infrastructure, that it might follow and emulate. Despite all the rhetoric and the photo ops and the paper exercises, the bad news continues to roll in with every GAO report, every inspector general's audit, with every congressional oversight hearing, with each day's newspaper accounts which each real-world test of government's computer systems security, no matter how recent, we continue to learn how bad the situation is.

For example, two reports released this year show little progress that Federal agencies have made in protecting critical cyberassets in the 3 years since the President issued his PDD-63. Essentially, we are still in the process of identifying the critical assets and their interdependencies, which raises the question, how can we adequately protect our most critical cybersystems when we haven't yet identified them all.

This is not to say that there have not been improvements in the area, and certainly there have been some, particularly at those agencies that have felt the sting of public embarrassment, but overall we are barely treading water; and unless we get serious about the effort, we will never keep up with the rapid advances of technology in this area which continue to reveal new ways to attack cybersystems.

The technology to get into our systems is advancing much more rapidly than the deployment of security to protect them, and in this increasingly interconnected world, we are either going to prioritize our resources better to meet this challenge, something that today Congress has not yet forced the agencies to do, or we are going to find ourselves in deep, deep trouble, and Americans are going to wake up angrier than you can possibly imagine to learn that in many cases their personal, sensitive data, which they shared not voluntarily, but involuntarily with the Federal Government, has been compromised and perhaps will be used in ways that they find very offensive.

This committee has both the responsibility and the authority to conduct oversight as to whether a nation's critical and computer systems are being adequately protected, and we intend to do that. And I want to thank you, Mr. Chairman, for taking this job and this assignment so seriously.

This is an extremely important hearing. If Americans are concerned about privacy and security on the Internet as they do commerce voluntarily, let me assure you their concern, as they share sensitive information with government agencies involuntarily, is even deeper, and our obligations here are much stronger.

Thank you for taking this seriously, and I yield back the balance of my time.

Mr. GREENWOOD. Thanks to the chairman for his statement.

[Additional statement submitted for the record follows:]

PREPARED STATEMENT OF DIANA DEGETTE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF COLORADO

I want to thank the Chair for holding this important hearing, and I want to thank our witnesses for being here today.

The positive aspects of advanced technology in communications go without saying. Enhanced inter-connectivity brings a whole new level of efficiency and speed to our systems.

The downside is that this same inter-connectivity can create vulnerability. I think a good analogy is when the gene pool of a certain species loses its diversity, a certain strain of virus can come in and wipe out the whole population because they all share the same vulnerabilities.

It is certainly eye opening to learn, as I did when preparing for this hearing, that the number of serious security breaches of federal systems is on the rise. Most unnerving of all is the knowledge that there were over 150 incidents of the utmost severity last year alone when an unauthorized user was able to gain complete control of a system within 32 federal civilian agencies.

The Government Information Security Reform Act, passed last year, appears to be a step in the right direction to evaluate government computer system weaknesses and then address the problems that exist. I expect that this subcommittee will be among the first to gain the results of the independent tests that are due to be completed by October of this year and again in 2002.

It is reassuring to learn that action has already been taken to evaluate the government's system weaknesses. I think the Clinton Administration deserves great credit for recognizing the growing threats to our nations security within this area, and taking steps to address the risk that poor federal computer security poses to our country. The Executive Order in 1996 that established the President's Commis-

sion on Critical Infrastructure Protection (PCCIP) was a tremendous step in officially recognizing this growing problem and bringing the public and private sector together to address it.

In 1998, a Presidential Directive was issued to have federal officials to create and implement a strategy for protecting the nations' critical infrastructures, which was another crucial step for the security of our country.

I am glad to learn that the new Administration is taking this issue seriously and am anxious to learn more about its plans to continue this important work and who will be in charge of coordinating this effort within each agency.

Thanks again to the witnesses for coming, and I look forward to hearing the testimony.

Mr. GREENWOOD. If there are no more opening statements by members, I would like to turn to our cybersecurity penetration demonstration and welcome Mr. Glenn Podonsky, Director of the Department of Energy's Office of Independent Oversight and Performance Assurance, and his excellent team of cyberexperts to this hearing. And I thank you for putting together this demonstration for the committee.

Mr. Podonsky, although you and your team technically are not witnesses today and are not testifying before the subcommittee, it is our general practice to swear in all persons who appear before the subcommittee; and if you and your team have no objection, I would like to do that now. I ask that you rise and raise your right hand.

Do any of you have any objections to testifying under oath?

Seeing none, the Chair then advises you that under the rules of the House and the rules of the committee, you are entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony?

Mr. PODONSKY. No.

Ms. MATTHEWS. No.

Mr. BELLONE. No.

Mr. HUSTON. No.

Mr. PETERSON. No.

Mr. GREENWOOD. In that case, would you please rise and raise your right hand, as you already have.

[Witnesses sworn.]

Mr. GREENWOOD. You may be seated and we recognize you, Mr. Podonsky, and look forward to your demonstration.

TESTIMONY OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE, ACCOMPANIED BY, JASON BELLONE, FORMER MEMBER OF THE COMPUTER ANALYSIS RESPONSE TEAM, FEDERAL BUREAU OF INVESTIGATION; KAREN MATTHEWS, FORMERLY WITH COMPUTER FORENSICS LABORATORY, U.S. DEPARTMENT OF DEFENSE; BRENT HUSTON, AUTHOR OF BOOK ON HACKPROOFING; AND BRAD PETERSON, DIRECTOR, OFFICE OF CYBER SECURITY AND SPECIAL REVIEWS, U.S. DEPARTMENT OF ENERGY

Mr. PODONSKY. Thank you, Mr. Chairman. We appreciate the opportunity to appear before this subcommittee for the sole purpose of demonstrating the cyberpenetration techniques employed by my office. As you are aware, my office provides the Secretary of Energy with an independent view of the effectiveness of Department poli-

cies, programs and procedures in the areas of cybersecurity, safeguard security and emergency management.

Today, my staff will provide a brief demonstration of our cybersecurity penetration capabilities. With me for the demonstration today are Mr. Jason Bellone, formerly with the FBI's computer analysis response team; Ms. Karen Matthews, formerly with the Department of Defense computer forensics laboratory; Mr. Brent Huston, author of a soon-to-be-published book on hack-proofing your e-commerce Web site; and Mr. Brad Peterson, my Director of the Office of Cybersecurity.

Our cybersecurity office maintains a continuous program for assessing Internet security to identify vulnerabilities that hackers and others could exploit. As part of the program, we continuously attempt to penetrate the DOE cybercommunity. We use this—we do this by using off-the-shelf software of hacking programs that are available to virtually anybody. Using these tools, we have been successful in identifying numerous vulnerabilities on DOE cybersecurity programs, and I am pleased to report, at the same time, those have been largely corrected by the Department.

We will take a few minutes to demonstrate the results of some actual inspections that have taken place over the last 6 months in order to show you the hacking techniques that we use and others employ. After the demonstration, we would be happy to respond to questions about the demonstration.

Let me now introduce Mr. Jason Bellone to lead the demonstration.

Mr. BELLONE. Thank you, Mr. Podonsky.

Mr. GREENWOOD. Why doesn't it surprise me that it is the youngest member of the team?

Mr. BELLONE. We are very proud to present our cybersecurity laboratory to you today. Although it is small in presence here, this laboratory is a comprehensive suite of headquarters, regional and mobile assets that we use, in effect, to attack and subsequently performance-assess the Department's information systems. It is our goal here to provide as much realism as possible to illustrate our cybersecurity penetration capabilities. The demonstration should give you an inside look at our process, and at the same time, I think you will see that the demonstrations will demystify the attacker process.

Let me highlight two points before I begin. First, each demonstration you will see derives from a real penetration test conducted against government sites within the past 6 months. Sites, however, will not be mentioned by name.

Second, all tools demonstrated are real, meaning employed as utilities by the attacker community. Some of these products are commercial. All are available downloads from the Internet and most are free. Nor will they be mentioned by name.

When we assess, we don't use rubber bullets and paint pellets. To the greatest extent possible, we use the same process, tactics and tools as an attacker. This process I refer to here is the attacker's modus operandi; hence, it is our modus operandi. We will follow this process throughout the demo, about one level of detail away from teaching you how to attack a system. So don't try this at home.

Without further delay, let's begin the demonstration.

We will start with footprinting. Footprinting is a 50,000-foot view, a snapshot, a bird's-eye view of your targets. It is anonymous. It is unintrusive. It is generally undetected. It is basically reconnaissance to gather a lay of the land. The ultimate goal is the who, the what and the where of the target.

I will turn your attention to the demonstration screen. The following demo will illustrate a utility, again freely available on the Internet, that will graphically depict the who, the what, the where of the target. Although this operation was conducted from Maryland, the source of our efforts appear to come from Tampa, Florida. I will refer you to line one of the table.

The table represents the path that our data flowed from, the launch point which was redirected from Florida to Maryland. In this case and only this case, I will tell you that we are looking at the Department of Energy's Web site for the purpose of illustration. The analysis section indicates the type of system of the target. This is the basic idea of what we are looking at, so what we have here is the who, the what, the where data collected. We are ready to move on to the second step of the process, which is scanning.

The scanning process enables us to generate our target, our target list, and develop an attack plan. The scanning operation employs hundreds to thousands of agents acting as virtual detectives checking the target systems for specific vulnerabilities. Each virtual detective reports its findings back to the attacker. The probing process emulates hostile operations and searches for known vulnerabilities.

The data base of vulnerabilities and exploit change daily. At the present time we test for over 900 vulnerabilities. Importantly, the scanning operation can be conducted with what we call "low and slow," which means covertly without detection. The end result is a vulnerability profile, or intact plan ultimately.

The next demonstration will show you exactly what the digital detectives delivered to us from an assessment we conducted a few months ago. I will again turn your attention to the demonstration screen.

These results represent the output of a very robust scanning effort directed at one of our sites. This was a source of our attack plan.

The significance of what you are looking at is this: The red icon represents the presence of a high-risk vulnerability, meaning it is probable for the vulnerability to result in system compromise. The yellow represents a medium-risk vulnerability that equates to a medium probability of system compromise. Let me drill down one level of detail to help you understand what you look at.

If I click the red icon, the high vulnerability icon, I can drill down to understand the exact nature of the finding. The detail supports a focused attack and later a corrective action.

The attack name is clear. It reads NBTDIC. More importantly, the description reads as follows, a share that requires only a password may be compromised using a dictionary file. Put simply, it details exactly what we need to do to focus our attack.

Our third example is a separate product that may serve in a similar capacity. In contrast to the commercial product we demoed,

this is a free utility. You will notice the presentation is similar, red equals high risk, yellow equals medium risk.

Something interesting to note here: In the upper left-hand corner is a summary of the findings. It is quantitative, tells us how many targets, how many vulnerabilities, how many warnings. Let me point out, there have been instances where the scan results did not yield significant vulnerabilities and, hence, the process can stop there. So each step is requisite for the next step, and with that we are on to enumeration.

As the scan results identify specific vulnerabilities for specific targets, we use this data to concentrate our efforts for more intrusive probing. The goal is to refine the attack plan with information about user accounts, file-sharing and system characteristics.

The next demo will show you how to use the scan data to concentrate efforts and probe for more valuable information. I will again turn your attention to the demonstration screen.

This utility enables us to probe for specific information relating to the scan results. The list has several possible targets. You can see that they are over 20 targets at the moment. So, next, although over 20 exist, we are going to focus on one. We have a game plan for attack then, to gain access to a user C drive. So—to remotely gain connectivity to a user's C drive over the Internet.

So with footprinting, scanning, and enumeration data in hand, we are ready to gain access to the system. The demo you are about to see is a playback of the exact same exploit that we used in the course of our assessment; the process, the tools and the data to include the password are directly from the assessment. The demo is technical, so I am going to narrate as we go through it, so you will understand what you are about to see. Keep in mind, our goal here is to run an attack on target X to gain access to the user's C drive. We will begin the demo.

This is Step 1. This is collecting basic configuration data. We use this data to enter into our utility, basically an attack utility, that will be used to crack the password. You will see that it is iterating through special characters, through letters, through numbers and so forth. It goes one character at a time; and for the purpose of this demo, we did select out of our set a four-character password. Again, it is original password from the site.

We have I, and we have A—still moving through, lasts only a few seconds—I-A-E, and you can see it is almost there.

We now have password in hand, so we move on to step three. Step three is to use that password to connect across the Internet to the user's drive. We enter the password and, voila, across the Internet, we have total access to this person's hard drive.

At this point, we can load anything we want or we can download anything we want. In particular, here, we are going to load something called a key stroker logger, and we are going to download a sniffer. We could equally upload the person's password file at this point. So for step five we will move on to escalating privileges.

As you could see from the demo, we gained unrestricted access to a user's hard drive, but an attacker would never stop here, nor do we. The idea now is to discover how far can we go, can we propagate throughout the network?

What you will see next is, we will crack a password. So with this foothold, we have downloaded the password file. The password cracking demonstration uses a password file captured from exploits similar to the ones we have demonstrated. The demo will highlight the fact that cracking passwords is simply a matter of time.

The tool you are about to see is designed to serve as a password auditing tool; that is, it is to check a department's password policy, eight characters, nine characters and so forth. It is publicly available and widely used in the information security community. Needless to say, it can have alternative uses to a malicious user.

Before we begin the demo, let me explain what you will be looking at. In the first column, that is the user name. When you log in, generally you enter a user name and a password. So that would be the user name, and the columns that are empty, those will be where passwords appear. It is empty at this point. At the blink of an eye you will start to see passwords appear. In the far column, that's the encrypted representation of the password. Let's start to crack.

We saw, at the blink of an eye, 25,000 words in the English dictionary and about 5 million tries occurred in a second. Less than a minute will pass for us to have the super-user password. We talk about root, super-user, administrator; bottom line, complete and utter control over the system. We will let it go for a moment. It is very far along. You see administrator, and you see it says MOTOROL. We are about two characters away from its completing. We find that we get to this point in under a minute most of the time.

You also notice that it is telling us that they are not under eight characters. However, this is still not compliant with policy. So you can use this to support policy programs that may exist for a department.

So it is completed. We now have super-user privileges. We will move on to the next demonstration.

You recall that we were able to upload both a key stroke logger and a sniffer to the target's hard drive. Commonly, we install the logger to capture the user's monitoring log in session. When you come in in the morning most likely you check your e-mail and so forth. The idea for what we do is, we load it that night so that we can catch what you do in the morning.

I refer you to the demo screen for a large picture, fairly hard to decipher, and that is because every key—escape, control, delete—is captured. It also runs in stealth mode, unknowing to the user, very hard to detect, and all of the results go to a text file which the attacker can bring to their system. Embedded between all of those escape keys and tab keys actually are passwords.

Of course, an attacker doesn't stop here either, nor should we, so we will go on to pilfering.

A sniffer is a stealth utility that will act as a wiretap, a wiretap that will listen to traffic traversing throughout the network. The idea of pilfering is to turn a compromised target into a listening device to capture not only what you are typing, but also what your peers are doing. Clear text passwords, e-mail correspondence, documents are all routed to the original recipient and, at the same time, rerouted to the attacker. In many cases, we have used this

to propagate our control to other areas of the network. This courtesy, with small footholds, escalating privileges and pilfering, enables us or an attacker to gain more and more control in the network.

The next short demonstration will demonstrate how a freely available tool can turn your machine into a secret listening device. Let me set up what you're looking at here.

I mentioned wiretap as an example. This is one snippet, 1 second from a wiretap, so to speak; and the purpose of this is to highlight that we indeed have user name and password. So we have gone from an exploit on a local machine to finding a way further on the network to other machines now. That is the point of pilfering.

We move on to covering tracks. Covering tracks is hacker 101. Hackers don't want to get caught. We do not employ this tactic as part of our process so that we can work with the sites to engage in what we call "post-incident analysis." Simply put, we leave our traces to enable the site and us to collaborate to understand the nature of the attack.

The following demo will demonstrate yet another freely available tool, erasing the traces of an attack with a few button clicks. What will be important to recognize here is that you will notice that it is only the traces of the attacking activity that are deleted. So a systems administrator would never be aware of what happened because all of the other logs, those that are from a normal conduct of a computer, would still be there. A button click, the traces are gone. Let's move on to back doors.

For the following demo I will submit this machine. Karen will do the heavy lifting here. Although this machine is separated by 20 feet of cable, we have executed the exact same exploitation with hundreds to thousands of miles of separation between our lab and the site. The message is clear that ownership and control of a resource is, to the fullest extent possible, in many cases more than the user. The goal is to make a key that only you can use to enter, create accounts, plant remote control services and to install Trojans. I will now start the demo.

Let me set the scene again here. Imagine yourself working in front of this screen, doing normal business work wherever—anywhere in the world, for that matter, okay? We have exploited this system unknowing to you, and we are now going to take over control by doing things like change colors. So you are sitting there and this is happening to you, okay?

The other thing we are going to do is, we are going to eject the CD on you—again, from 3,000, 2,000, 1,000 miles away—and the other thing we might do, just to harass you a little more, is to hide icons. There we go. The point being—these are visual examples; ultimately, it is complete control.

A popular news organization reported about this tool, and let me quote: "he or she can access your files, monitor your key strokes, move your mouse around the screen. If you have a Web cam, they can watch what you are doing. If you have a microphone, they can listen to you. It is complete power."

This concludes the demonstration portion of our testimony. In closing, I will highlight the end product of this capability.

The essence of our capability is our final product. Our product encapsulates every element of what you have just seen—process, tactics, tools, every vulnerability and exploit. Along with meticulous note-taking and recordkeeping, we deliver all of this information to the site in a user friendly, Web-based CD-ROM. So anything and everything that is collected, yellow sticky and so forth, is given to the site for corrective action. I know you are also familiar with our paper product, which combines the technical elements with the policy, program and procedural analysis.

Thank you.

I will now offer our technical team for technical questions, as well as Mr. Podonsky and Mr. Peterson, who can entertain questions about our program.

Mr. GREENWOOD. Thank you. Now, I know why I can't open my e-mail in the morning.

I don't know if you are able to answer this in anything like a brief response, but what are the fundamental things that agencies and Federal entities ought to do to protect themselves from this kind of assault?

Mr. BELLONE. It is due diligence. This—what you are seeing here is such a dynamic process that it is a snapshot in time when we do an assessment. The fundamental core of doing this is to have program, policy, procedure and technology working together. That is why the scope of our assessments is what is important, that we do the technical elements, but at the same time, we have a team who looks at policy, looks at programs, looks at procedures. We put it together so that we can understand the health of a program and how they are able to sustain the program. It is the sustainability that is most significant.

Mr. GREENWOOD. So what I hear you saying is that you are never finished with your security precautions. You can't build a firewall or create air space and stay permanently fixed. You always need to be——

Mr. BELLONE. The quote that I think about is, "as technology evolves, sneakiness finds new ways of expression;" and that's exactly where we are. We can assume technology will evolve, especially in this growing field of information technology. Hence, the task is always ahead of us.

Mr. GREENWOOD. That is a fascinating, fascinating demonstration.

Are there questions from the members for the technical panel here?

The Chair recognizes the chairman, Mr. Tauzin.

Chairman TAUZIN. Thank you very much.

I simply want to put what you have told us in layman's terms a little bit. Am I correct in that, with this demonstration, you have shown us how a hacker cannot only compromise the system but take it over and actually control the information on that system? Is that correct?

Mr. BELLONE. Yes.

Chairman TAUZIN. You have shown us how someone who could compromise, let's say, a third-party payment system at HCFA to get into that system—how they might not only gather the informa-

tion that's in that system about patient's health care and problems, but that they might even alter the information on that system?

Mr. BELLONE. Absolutely.

Chairman TAUZIN. So that I take it your answer is, yes, right?

Mr. BELLONE. My answer is yes.

Chairman TAUZIN. So the person who is using the systems you have demonstrated can actually change the medical condition or the treatment profile or the payment requirements of that system; is that correct?

Mr. BELLONE. That is exactly correct.

Chairman TAUZIN. And, therefore, compromise the integrity of the payment system?

Mr. BELLONE. Absolutely.

Chairman TAUZIN. I can envision incredible fraud opportunities with that scenario, is that right, as well as privacy problems?

Mr. BELLONE. You can assume that with what we have shown, an attacker can gain more privileges than the user has.

Chairman TAUZIN. Say that again, "An attacker can gain more privileges than the user." What do you mean by that?

Mr. BELLONE. What I mean is that once you exploit it, you can deny them service to that resource.

Chairman TAUZIN. So you can not only take charge of their operation, you can make it more difficult for them to actually use it themselves?

Mr. BELLONE. Absolutely.

Chairman TAUZIN. You can deny them total use, if you want, of these systems?

Mr. BELLONE. Absolutely.

Chairman TAUZIN. You also indicated—obviously, I am just using health care systems as an example for us to understand this technology, but this, in the case of an energy lab, might explain how someone might get in and compromise, with espionage intent, not only the information in that lab, but you might do it from across the world.

You don't need necessarily someone working in the lab; is that right?

Mr. BELLONE. To a certain extent. The one thing that I think the Department of Energy recognizes is, given that risk, there are certain assets that they are not willing to subject to that risk.

Chairman TAUZIN. Well, let's hope so.

Mr. BELLONE. Yes.

Chairman TAUZIN. But we have some confidence problem with that.

Yes, sir.

Mr. PODONSKY. Also the fact that we exist as an organization to continue doing these penetrations is a compliment to the current Secretary and the Department because we are allowed, without legislation, to go anywhere that we need to and report on anything that we find.

Chairman TAUZIN. On the technical side again, the last thing you said was quite disturbing as well, that if you had a camera, once this system is compromised, that you take over that camera, that you can actually watch activities in that room in front of that screen; is that correct?

Mr. BELLONE. Absolutely.

Chairman TAUZIN. And if you have a microphone, which most computers do, you can, with this technology, install your sniffer and actually listen in on all conversation inside that room; is that correct?

Mr. BELLONE. Absolutely. If the machine has a microphone, that is the case.

Chairman TAUZIN. And unless all the Federal sites in which sensitive information is being discussed are protected against this technology, anyone from around the world using it could enter any room where sensitive conversations are being held and eavesdrop on those conversations without a court order covering their tracks, without anybody ever knowing they have done it; is that correct?

Mr. BELLONE. To a certain extent, it is correct.

What I could say is that in some environments they look harder at things like hardware, the presence of microphones and so forth, and so that is looked very carefully upon. In other environments where there is less, where there is not the presence of sensitive information, it is more likely that that may be the case.

Chairman TAUZIN. But it is a problem. Unless the Federal official who is operating in front of that computer screen which has camera and microphone capabilities is aware of what you have just shown us, if he has no awareness of it, if it is not a priority item in his thinking or her thinking that day, that conceivably those systems can be compromised in the way you have demonstrated and the conversations, the actions even in that room can be in someone else's domain, unknown to the Federal officials involved.

Mr. HUSTON. That is correct, sir, but you have to realize that it should never get that far. There should be defensive measures installed in these systems to prevent that from occurring long before that ever becomes a risk.

Chairman TAUZIN. That is, of course, the next question.

You know, I have raised in the opening statement the concern that enough of our Federal agencies are not keenly aware, we have not yet made them keenly aware nor instructed them nor appropriated funds for them to install these defensive systems. Is that generally correct as well? Who can answer?

Mr. PODONSKY. Well, we are better off to keep focus on what we do know about the Department of Energy. On the technical side, we don't know what all the other agencies are doing, but we do know that because of some very good reasons, the Department was very motivated in the last 2 years to really focus on cybersecurity.

Chairman TAUZIN. Something called public embarrassment, I think.

Mr. PODONSKY. That often helps.

So to answer your question, from our standpoint, as we pointed out here, not only do we continue to probe, but the people who are responsible for filling the vulnerabilities that we find are actively doing that as we speak on a regular basis.

Chairman TAUZIN. And I guess, as a final question, these technologies are also available for private snooping and private compromising of homes and businesses across America; is that correct? Unless Americans are aware, keenly, of the capabilities of these systems and take as much concern about installing defensive sys-

tems, their private homes, their most private conferences, in many cases their most private spaces and activities can be easily compromised by someone invading their home through these devices and literally listening in and watching the most private of circumstances of Americans in their personal and business lives; is that correct?

Mr. HUSTON. That is correct. However, awareness is the primary means of defense against any security threat, and much like a physical security threat, where you have started to see the evolution of homeowners installing alarm systems and other threat and risk mitigation strategies, I think you will see a growth in that marketplace, as well, for cybersystems.

Chairman TAUZIN. Thank you, Mr. Chairman.

Mr. GREENWOOD. Let me just ask a question about motivation.

Obviously, we know that there are some hackers who do this for the sport of it, just to see what they can do, and they may or may not have nefarious intentions other than to sneak in and see what they can do. But what nefarious opportunities are there once you get in?

In other words, I assume a lot of people wouldn't get all the way there just to hide your icons or change the colors on your screen; that they would be there to—is there a market for the information? Can you get information and then sell it? Is it a question of compromising and destroying internal systems for strategic purposes?

Talk, if you would, briefly about some of the motivations for doing this.

Ms. MATTHEWS. I think the answer to your question is all of the above and then some.

There are over 100 countries that have some sort of information operations capabilities, and you saw what we could do with publicly available software and hardware. If you could imagine them turning their expertise and resources to debunking those information and operations, you can imagine what damage that could do. So the motivations are various, depending on whether it is a teenager or whether it is a nation-state or a terrorist organization that has motivation behind them.

Mr. GREENWOOD. And given the ability to cover tracks, it is safe to say that this has probably happened to Federal systems, and we don't know what was done, have no way of knowing what was done? They could have covered the tracks and left no trail whatsoever?

Mr. BELLONE. Part of strength and defense is having an effective intrusion detection system—and I emphasize the word "system," because what we showed you is covering tracks at a very micro level. When we assess a site, one of our topical areas is intrusion detection systems, meaning their ability to respond to an event and provide that for an investigation, if you will. That is a critical component of detecting that level of activity. Sure, there are point-and-click tools available to vanish yourself from one machine, but with a very comprehensive system of alarms, you can still detect the activity.

So there are defense elements that are available.

Mr. GREENWOOD. Mr. Strickland, do you have questions for the panel?

Mr. STRICKLAND. No, sir, but I want to thank the panel. They have been very stimulating, and I am sitting here wondering what their IQs must be.

Mr. GREENWOOD. We can assume it is higher than ours.

Mr. Davis.

Mr. DAVIS. Thank you. You can never have 100 percent protection in an information system; do you agree with that?

Mr. BELLONE. That is correct.

Mr. DAVIS. Information security best practices really means using effective risk management in their implementation. How do you collaborate with your clients to assist them in meeting those objectives?

Mr. PETERSON. We have—as part of our process, we do the technical performance testing, what Mr. Bellone has shown you today. We then go in with our programmatic team and we take a look at their processes, and one of the key ones would be the risk management process, you know, does the site understand the threat. Then you do a risk assessment, understanding your critical systems and your critical information need protection. You then devise risk mitigation strategies and a protection strategy as well.

You implement those, and then there is going to be some residual risk left over. What we do then is, we go in to see, do you understand your residual risk, has there been an appropriately designated official—has that person accepted that risk. That is what we look for.

Mr. DAVIS. Thanks.

Mr. GREENWOOD. Ms. DeGette.

Ms. DEGETTE. Thank you, Mr. Chairman.

I want to follow up on the full committee chairman's questions about, if you had microphones and video capability in computers. I would assume that for someone to be able to intercept that, the computer would have to be on at that time. And is that a yes?

Mr. BELLONE. That is correct.

Ms. DEGETTE. And I would also assume that many meetings that take place where secret information is discussed are not in people's cubicles or offices where their PC is on, but rather in a conference room or some other venue. Would that be correct?

Mr. BELLONE. Absolutely.

Ms. DEGETTE. And in those venues, in your experience in your agency, are there computers running in those rooms at the time those meetings are taking place? I am trying to figure out how real a threat this really is.

Mr. BELLONE. In the sensitive realm, there is a very clear accreditation process that looks at the room—the nature of the room, the hardware, the software and so forth. So it is very much a controlled environment, and because there are so many checks and balances and procedures and signatures and so forth, generally the process resolves or reconciles those kinds of concerns.

Ms. DEGETTE. And that is happening under current DOE protocols?

Mr. BELLONE. Accreditation process.

Mr. PODONSKY. Yes.

Ms. DEGETTE. And what about the training of personnel, are personnel currently, under current protocols, trained about the risks of interception of verbal communications?

Mr. PETERSON. It is part of what we look at in our programmatic review, we look for annual training of users—obviously more detailed training down to the systems administrator level, managers—making sure that they understand their roles and responsibilities, making sure that the site has good procedures that actually push policy down from the broad national perspective down to the working level.

Ms. DEGETTE. Well, these particular concerns that Mr. Tauzin was expressing are—is that part of your current training for personnel about the risks of hackers coming in and actually being able to intercept visual or verbal discussions? Is that a policy right now?

Mr. PETERSON. Again, that is part of the risk assessment process that is evaluated at the site level for each individual network. You know, depending on what information they have, again it is going to drive the level of concern. Again, that is a process at the site level.

Then that feeds into the training based on, we know we have these risks, we need to inform our users and our systems administrators.

Ms. DEGETTE. I understand what your general protocols are, but specifically, are people advised of these risks?

Mr. BELLONE. One thing that comes to mind, we run through computer-based training in yearly training sessions that go over counterintelligence and cybersecurity, and the cybersecurity awareness training covers these elements. They talk about the exploit or attacker threat. That is required yearly.

Ms. DEGETTE. Now, let us talk for a minute about classified systems. By the way, I apologize, I missed your demonstration. I was caught in the cherry blossom traffic, I think.

But apparently, according to Mr. Strickland, we are never turning on our computers again because of the risk of people getting our information, and I want to know how very real the risk is with your Agency? Are the classified systems at your Agency connected to the Internet?

Mr. PETERSON. We take a very close look at that. With classified systems, there is either an air gap between the Internet and the classified system or NSA-approved encryption.

Ms. DEGETTE. So some are connected to the Internet, but there are protections that you believe would be effective in place?

Mr. PETERSON. Yes.

Ms. DEGETTE. How many of the classified systems, what percentage of your classified systems are connected to the Internet?

Mr. PETERSON. I am not sure if we can provide a good number for that.

Ms. DEGETTE. If you can supplement your answer in writing, I would appreciate it. Mr. Chairman, thank you.

[The following was received for the record:]

The Department has one classified system connected to the Internet. However, all classified information that is transmitted over the Internet is protected using an encryption device approved by the National Security Agency.

Mr. GREENWOOD. We thank you for that mind-bending demonstration. You are excused, and we will bring up the next panel. Thank you again.

The Chair calls the witnesses, Ms. Sallie McDonald, Assistant Commissioner, Office of Information Assurance and Critical Infrastructure of the U.S. General Services Administration; Mr. Ron Dick, Director, National Infrastructure Protection Center of the FBI; and Mr. Tom Noonan, President and CEO of Internet Security Systems.

The Chair would ask unanimous consent that the gentleman from Georgia, Mr. Isakson, be given permission to sit at the table and introduce his constituent, Mr. Noonan.

I am going to have Mr. Isakson introduce Mr. Noonan first, and then we will turn to Ms. McDonald for her opening statement.

Mr. ISAKSON. I commend the chairman and members of the committee for looking into an issue of major importance to the U.S. Government. It is also an issue of major importance as well to the private sector throughout this country.

I am particularly pleased to have the honor to introduce a citizen of Atlanta, Georgia, Mr. Tom Noonan, Chairman and CEO of Internet Security Systems, whose software development, remote management of security systems, education and consulting is sought worldwide. ISS is a company that has offices in Asia, Latin America, Middle East, Europe and throughout North America. They have over 6,000 customers in the United States of America in the management and security of their network systems.

To talk about the importance of the software that they developed and the remote management that they have, today 21 of the top 25 banks in the United States of America are clients of ISS. The top 10 telecommunications companies in the United States of America are clients of ISS, and 35 government agencies in this country, or possibly worldwide, are clients of ISS.

But probably the best compliment that I can pay to Mr. Noonan is that 2 years or 3 years ago, following my election to Congress, I sought the opportunity, because of my business experience and knowing the importance of technology, to develop an advisory board of individuals to help me deal with the myriad of privacy and safety and security issues that deal with the Internet and technology. Tom Noonan's name was consistently mentioned as the paramount authority on security systems in Atlanta, and, in fact, in the United States. It is an honor and privilege for me to introduce him. I am going to apologize that I have to leave this table, but I have the intellectual capacity to be a Congressman; I am not sure that I have the capacity to sit at this table with these individuals, and I do not want to confuse anyone here. I thank the chairman.

Mr. GREENWOOD. I thank the gentleman. The Chair recognizes Mr. Davis.

Mr. DAVIS. Mr. Isakson, you missed one item in that introduction. That is, his company has a strong presence in Herndon, Virginia. Welcome.

Mr. GREENWOOD. The Chair recognizes Ms. Sallie McDonald for her testimony.

TESTIMONY OF SALLIE McDONALD, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE, U.S. GENERAL SERVICES ADMINISTRATION; RONALD L. DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER; AND TOM NOONAN, PRESIDENT AND CEO, INTERNET SECURITY SYSTEMS, INC.

Ms. MCDONALD. Good morning, Mr. Chairman and members of the committee. I am the Assistant Commissioner for the Office of Information Assurance and Critical Infrastructure Protection. My office is a component of GSA's Federal Technology Service under which the Federal Computer Incident Response Center operates.

We wish to thank you for the opportunity to offer testimony pertinent to the state of security for government information technology resources. The Federal Computer Incident Response Center, or FedCIRC, is a central coordination activity for dealing with computer security-related incidents affecting computer systems within the Federal civilian agencies and departments of the U.S. Government.

As government industry system interconnectivity increases, the boundary between the two becomes more difficult to define and in some cases they simply do not exist. Any security weakness across the Internet has a potential of being exploited to gain unauthorized access to one or more of the connected systems, including those of government. Reports indicate that numerous countries have or are developing information warfare capabilities that could be used to target critical components of the national infrastructure, including government systems. The National Security Agency has determined that potential adversaries are collecting significant knowledge on U.S. information systems and also collecting information and techniques to attack these systems.

Since October 1998, FedCIRC incident records have shown an alarming trend in the number of attacks targeting government systems. Overall, 376 incidents were reported in 1998, affecting 2,732 Federal Government systems.

In 1999, the figure had risen to 580 reported incidents affecting 1.3 million systems. By 2000, reported incidents numbered 586; and those incidents impacted over 576,000 government systems.

Although these numbers are alarming, it should be noted that they reflect only those reported incidents and do not include statistics on the estimated 80 percent that go unreported. Studies indicate that the lack of reporting is not due to an organization overlooking its obligation to report, but rather a sign of the organization's inability to recognize that its systems have been penetrated. The increase in the number of route compromises, denial of service attacks, network reconnaissance activities, destructive viruses and malicious code, coupled with advances in attack sophistication, pose immeasurable threats to government systems and the critical missions and services they support.

With the rapid transition to a paperless government and increasing dependence on e-government solutions, the focus on secure technology approaches must be a priority. We in government cannot afford to overlook our inherent responsibility to protect sensitive information from unauthorized disclosure. The unprecedented growth in technology is driving government to implement

capabilities and services so rapidly that security concerns are often overlooked.

Mr. Chairman, my brief summary today only begins to touch on the most significant information security challenges we have before us. The complete text of my testimony describes in greater deal the current and growing threat to the Federal information infrastructure. I trust that you will derive from my remarks an understanding of the cybersecurity issues, and also an appreciation for the commitment that those in the FedCIRC and participating organizations share for the protection of components of our critical infrastructure. 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 defenses of the Federal information technology resources. Thank you.

[The prepared statement of Sallie McDonald follows:]

PREPARED STATEMENT OF SALLIE MCDONALD, ASSISTANT COMMISSIONER, OFFICE OF INFORMATION ASSURANCE AND CRITICAL INFRASTRUCTURE PROTECTION, FEDERAL TECHNOLOGY SERVICE, GENERAL SERVICES ADMINISTRATION

Good morning, Mr. Chairman and Members of the Committee. On behalf of the Federal Technology Service of the General Services Administration let me thank you for this opportunity to appear before you to discuss our perspective on the state of security for government information technology resources.

As you know we operate an entity known as **FedCIRC. FedCIRC stands for the Federal Computer Incident Response Center,** and is a component of GSA's Federal Technology Service. FedCIRC is the central coordinating activity associated with security related incidents affecting computer systems within the Civilian Agencies and Departments of the United States Government. FedCIRC provides security incident identification, containment and recovery services and works within the Federal community to educate agencies on effective security practices and procedures. FedCIRC's prevention and awareness program includes security bulletins and advisories, hardware and software vulnerability notifications, and vulnerability fixes.

With the recent enactment by Congress of the **Government Information Security Reform Act,** federal agencies and departments must report computer security incidents to FedCIRC. FedCIRC's role is to assist those federal agencies and departments with the containment of security incidents and to provide information and tools to aid them with the recovery process. In January, the Office of Management and Budget (OMB) issued implementing guidance on the new security act. In that guidance, OMB instructed agencies to implement both technical and procedural means to detect security incidents, report them to FedCIRC, and to use FedCIRC to share information on common vulnerabilities. Agencies were advised to work with their security officials and Inspectors General to remove all internal obstacles to timely reporting and sharing. Additionally, in October of last year, the Federal CIO Council worked with FedCIRC and developed procedural advice to agencies for efficient interaction with FedCIRC.

When an incident is reported to FedCIRC, we work with those involved to collect pertinent information, analyze it for severity and potential impact, and offer guidance to minimize or eliminate further proliferation or damage. Additionally, FedCIRC assists in identifying system vulnerabilities associated with the incident and provides recommendations to prevent recurrence. Moreover, FedCIRC works closely with the FBI's NIPC and the national security community to ensure that incidents with potential law enforcement or national security impact are quickly reported to the appropriate authorities.

As government and industry systems and network interconnectivity increase, the boundaries between the two begin to blur. This huge network of networks, known of course as the Internet, includes both government and private systems. In some fashion, through the Internet, all of these systems are interconnected. Thus, an inescapable fact of life in this Internet Age is that any risk associated with any part of the Internet environment is ultimately assumed by all systems connected to it. Any security weakness across the Internet has the potential of being exploited to gain unauthorized access to one or more of the connected systems.

Reports from the Department of Defense and other sources tell us that over 100 countries have or are developing information warfare capabilities that could be used to target critical components of the national infrastructure including government systems. The National Security Agency has determined that potential adversaries are collecting significant knowledge on U.S. information systems and also collecting information and techniques to attack these systems. These techniques give an adversary the capability of launching attacks from anywhere in the world that are potentially impossible to trace.

Since October 1998, FedCIRC incident records have shown an increasing trend in the number of attacks targeting government systems. Overall, there were 376 incidents reported in 1998 that affected 2,732 Federal civilian systems and 86 military systems. In 1999, the figure had risen to 580 reported incidents affecting 1,306,271 Federal civilian systems and 614 military systems. By 2000, reported incidents numbered 586, which impacted 575,568 Federal civilian systems and 148 of their military counterparts. Though these numbers are in themselves ample cause for concern, these numbers reflect only those *reported* incidents and do not include incidents that were not reported. Studies conducted by the Department of Defense as well as data collected from the broad Internet community by Carnegie Mellon University's CERT Coordination Center indicate that as many as 80% of actual security incidents go unreported. More importantly, perhaps is the reason incidents appear to remain unreported. In most cases incidents are not reported because the organization was unable to recognize that its systems had been penetrated or because there were no indications of penetration or attack.

Of course computer security incidents vary in degree of severity and significance. Many incidents, such as web page defacements, are seemingly insignificant and generally categorized as "cyber-graffiti." Typically, systems that are victims of defacement have one thing in common, an *overabundance of commonly known weaknesses* in their respective operating system and server software. Though the damage from such incidents may be small, the rising number of occurrences suggests a clear pattern of inattentiveness to security problems, especially those that might be easily resolved with publicly available software patches.

While these relatively minor incidents may amount to mostly nuisances, the more significant incidents are those associated with the development of sophisticated *attack methodologies.* Such attack methodologies involve the organized distribution of intrusion techniques across the Internet. So called "hackers", "crackers," mischievous individuals, rogue nations and even state sponsored attacks are all threats to systems in government and the private sector.

In particular, unauthorized intrusions into government systems containing sensitive information are also on the rise. In 2000, as I reported earlier, FedCIRC documented 586 incidents affecting government systems. 155 of those were reported from 32 agencies and resulted in **what is known as "root compromise."** A root compromise means the intruder has gained full administrative or "root" privileges over the targeted system. This means that any information or capability of the system is totally owned by and controllable by the intruder. With "root" privileges, the intruder can cover his or her tracks because the privileges allow them to alter system logs and thereby erase any evidence of intrusion activities. In at least 5 of the incidents involving a root compromise, access to sensitive government information was verified. For the remaining 150 incidents, compromise of any and all information must be assumed. Root compromises were also employed in 17 separate instances where the compromised systems were used to host and then launch attacks. Attacks of this nature are particularly egregious since they work to erode the public trust in government systems integrity while serving to openly demonstrate security vulnerabilities within government systems.

More recently, as a byproduct of the Y2K problem, a new type of attack has been gaining attention. This type of attack is known as the **"Distributed Denial of Service"** attack and is considered one of the most potentially damaging attack methods yet to be developed. The Distributed Denial of Service or DDoS attack simply overwhelms a targeted system with so much information that the targeted system cannot grant access to legitimate users. This attack can be particularly damaging when components of the critical infrastructure such as power grid controls, traffic controls, emergency and medical services are subject to a DDoS attack, since these attacks render their targets effectively inoperative. And if that is not enough, the DDoS attack, after first identifying and compromising vulnerable systems anywhere across the Internet, next deposits on those compromised systems hostile software capable of launching further attacks. Once in place, the exploited systems can then be orchestrated to simultaneously launch attacks on a predetermined target, flooding the target with more information than it is capable of processing. Ninety

three government systems were targets of DDoS attacks, many of which resulted in the disruption of critical government services.

Perpetrators continually scan the Internet to identify systems with weak security profiles or vulnerabilities. These *reconnaissance activities* focus on identifying the active services, operating systems, software versions and any protective mechanism that may be in place. Armed with this information, a would-be intruder can consult publicly available information repositories and references for vulnerabilities particular to their selected target. Then they can devise attack strategies with the highest probabilities for successful compromise. Port scans, probes, network mapping applications and commonly used network administration tools are typical resources used by an intruder to identify weaknesses in the chosen organization's infrastructure and to simplify the intrusion effort. Incidents reported by Federal agencies to FedCIRC during 1998 indicated a mere 157 occurrences. However in 1999 there was a significant jump in network reconnaissance activity to 1,686 occurrences. Although 2000 showed a slight decrease, the number of reported reconnaissance incidents still was 1,207.

The sophistication of **computer viruses** also poses a significant threat. While yesterday's viruses were destructive to files residing on a system, today's viruses come in many forms and self propagate by exploiting the advanced capabilities of modern-day software applications. Computer viruses may harbor capabilities to destroy both hardware and software. They may arrive in the form of so-called **"trojan horse"** code capable of capturing and transmitting sensitive information, user account data or administrator passwords. As legitimate software programs incorporate more advanced capabilities, those same capabilities are being harnessed to very destructive purposes. As we observed during the "Melissa" and "I Love You" viruses, a single email on the other side of the globe began saturating mail servers within a few short hours. The number of virus incidents reported by Federal agencies in 1998, 1999 and 2000 totaled 55, 35, and 36 respectively. Since anti-virus defenses are developed in response to a virus, there is a relatively significant period of time between the capturing of the virus code and the development of a defense. Considering the near-real-time communications capabilities available to a large percentage of the world population, microseconds can mean the difference between normal operations and system disruption.

Statistics compiled by Carnegie Mellon University's CERT Coordination Center show a definite correlation between the growth of software vulnerabilities and the number of reported incidents. From 1988 to present day, the number of vulnerabilities identified annually has increased from only single digits to well over 800. The number of reported incidents across industry and government closely track that of the vulnerabilities, from a meager few in 1988 to almost 25,000 as of the beginning of this year. These trends indicate that Internet connected systems are becoming increasingly vulnerable to attack and that defensive measures are not yet adequate to protect against exploitation of the vulnerabilities.

With the rapid transition to a paperless government and increasing dependence on e-government solutions, the focus on secure technology approaches must be a high priority. The unprecedented growth in technology is driving government to implement capabilities and services so rapidly that security concerns are often overlooked. The adoption of e-commerce solutions, e-government solutions and countless forms of electronic information exchange is in danger of moving forward without adequate consideration of the protection of the systems and the information they store, process or transmit. We in government cannot afford to overlook our inherent responsibility to protect sensitive information from unauthorized disclosure. The implementation of strategic defenses for the Federal Information Infrastructure can only be realized if we act promptly to establish the proper foundation for already overdue initiatives to combat these issues. Information sharing and collaboration on the part of all concerned is key to the creation of effective defenses. FedCIRC, in cooperation with every Civilian Federal Agency, Industry, Law Enforcement, the Department of Defense and Academia, has begun building a virtual network of partners to facilitate the sharing of security relevant information and ideas. Each week, the list of partners increases as more and more realize that this battle cannot be fought in isolation. Every contributing piece of information from a participating partner has the potential of unlocking a critical cyber-defense problem.

SUMMARY

Mr. Chairman, in my remarks here this morning, I have merely touched on the most significant information security challenges we face in this Internet Age dawning before us. My goal was to inform you and this committee about the nature of the cyber-security issues we face collectively as a nation. I also want to help you

appreciate the degree and level of commitment that those in FedCIRC and participating organizations share regarding the protection of the components of our Critical Infrastructure. We appreciate your leadership and that of the Committee in helping us achieve our goals and allowing us to share information that is crucial to the effective defense of Federal Information Technology resources.

Mr. GREENWOOD. Thank you.

Mr. Dick.

TESTIMONY OF RONALD L. DICK

Mr. DICK. Mr. Chairman, I am the Director of the National Infrastructure Protection Center which is located at the FBI. I want to thank you today for inviting me to discuss cyber-intrusion issues into government systems. Because of the impact that cyber-intrusions have on our national security, as well as the economic well-being of government and industries to provide vital goods and services to Americans, this is a very important topic.

I would ask that my full statement be entered into the record, and I will focus on a few brief comments.

Computer intrusions into government systems are a serious problem. In my statement, I cite that we have currently 102 pending investigations of government systems out of a total of approximately 1,219. But each case can represent multiple intrusions and multiple victims. Thus the caseload denotes a large number of incidents. That is the bad news.

The good news is that National Security Advisor Rice's recent statement at the Partnership for Critical Infrastructure for Security meeting indicated the administration's view that this is a high priority.

Let me briefly outline some threats we face and discuss a few examples that highlight the vulnerability.

Insiders have always been a major threat. Their motive is usually against a current or former employer. In many instances they do not need to be sophisticated because they do know the passwords, or controls are such that passwords are not changed routinely. Further, they have the greatest knowledge of how to defeat the system's internal controls.

In one case, a dismissed employee of the National Library of Medicine created a back door in the system through which he could alter and destroy data on the system. These intrusions were a threat to public safety, as doctors from around the world depended on the integrity of this information for diagnosis and drug prescriptions.

Computer virus writers have become a dangerous problem in the last few years. They write their programs, often just to cause mayhem in the networks. The result is that important systems are made or forced to come off-line for repairs. This is at a cost of billions of dollars; last year, as we all remember, the well known love letter virus which began in the Philippines but soon spread globally. The FBI and Philippine authorities were able to trace the virus back to its source, but because the Philippines lacked a cybercrime statute at the time, he could not be prosecuted.

Along with viruses, hacking cases are the best known. In February 1998, just as the Center was being established, we had one of the largest hacks ever of U.S. Government systems. Intruders had compromised hundreds of Department of Defense computers.

We initially thought it could be an attack from a foreign power. It turned out to be teenagers from California and Israel. Those teens have since been prosecuted by the U.S. Government; but it was a wake-up call regarding cybersecurity.

While the motive was less malicious in this case than others we had seen, it highlighted the potential for use of cyberspace to prepare the battlefield.

Let me touch further on national security threats. There are thousands of intrusions or attempts into government systems every year. Many of them emanate from abroad. We know many nations are developing information warfare capabilities, as well as adapting cybertools as information-gathering trade craft. That is about as far as I can go today, but this is an evolving area for us.

Let me talk about the response to these threats. In the middle of the 1990's, the Federal Government, as has been recognized already, recognized the potential dangerous problem regarding cyber-vulnerabilities.

In February 1998, the Attorney General authorized the creation of the National Infrastructure Protection Center. In May 1998, President Clinton authorized the expansion of Justice Department efforts to a full-scale National Protection Center. The Center's mission is for detecting, assessing, warning of, and investigating significant threats and incidents concerning our critical infrastructures. The NIPC is an interagency center. Of the 101 persons currently working in the Center, we currently have 18 detailees from outside the FBI, and two foreign detailees. The leadership of the Center comes from several agencies. The NIPC's Deputy Director is Rear Admiral James Playhall from the Navy, who is with us today. Over the last 3 years the Center has issued 82 warning products. Many of these products, such as the one issued last week on the "Lion Internet Worm" are issued before any attacks occur.

These warning products are sent to our Federal partners, as well as State and Federal law enforcement, international partners with whom we have connectivity, the information sharing and analysis centers, and others in the private sector so as to enhance security worldwide.

What makes the NIPC unique is that we have access to information from law enforcement sources and investigations, the intelligence community, international sources, private sector contacts and open sources. No other entity has access to such a complete range of information.

In cyberspace, we all look the same as has been pointed out here today in the demonstration. Thus, investigations is an important component of what the center does. Finding out the origin of an intrusion and who is sitting behind that keyboard is a huge challenge. What makes the NIPC unique is that through the FBI, we have access to both criminal and national security authorities to conduct such investigations. As an interagency center, we can coordinate our investigative efforts more efficiently. If the intruder is overseas, we can use our partners regarding investigations and prosecutions through our legal attaches in over 40 countries around the world. Once we have determined the facts regarding the attack and the identity of the attacker, we can confer with the Depart-

ment of Justice, and just as importantly, policymakers, to fashion the appropriate response.

That response may be criminal prosecution or it might be diplomatic, intelligence, or military action, or a combination of all three of those things.

In summary, I must stress that cooperation lies at the heart of everything that we do within the Center. We are actively engaged with our Federal partners, domestic law enforcement, international agencies, the private sector, and our international counterparts across the globe. Without cooperation and information sharing, we cannot hope to come to grips with this problem. We have made a lot of progress, but much work remains to be done. Thank you.

[The prepared statement of Ronald L. Dick follows:]

PREPARED STATEMENT OF RONALD L. DICK, DIRECTOR, NATIONAL INFRASTRUCTURE PROTECTION CENTER, FEDERAL BUREAU OF INVESTIGATION

Representative Greenwood, Members of the subcommittee, thank you for inviting me here today to speak to the important issue of intrusions into government computer networks. The problem is serious. The Department of Defense reports thousands of potential cyber attacks launched against DoD systems. GAO reports that "in 1999 and 2000, the Air Force, Army, and Navy recorded a combined total of 600 and 715 [serious] cyber attacks, respectively." This does not even consider attacks on civilian agencies. Two weeks ago National Security Advisor Condoleezza Rice stated that "The President himself is on record as stating that infrastructure protection is important to our economy and to our national security and therefore it will be a priority for this administration."

Dr. Rice also stated during that same speech that, "We have to maximize our resources and energies by making sure that they are focused, instead of allowing them to be dissipated through dispersal." The need for a coordinated interagency approach to address intrusions into government networks was one of the principal reasons for having established the National Infrastructure Protection Center (NIPC). When the NIPC was founded three years ago, it was during one of the largest intrusions ever into U.S. government systems. The lessons learned from that intrusion and from the response to it have helped shape the NIPC.

Let me provide you with a snapshot of our caseload on government intrusions. Currently we have 102 cases (of a current total of 1,219 pending cases) involving computer intrusions into government systems. This includes intrusions into federal, state and local systems, as well as the military. It should be noted that a single case can consist of hundreds of compromised systems that have experienced thousands of intrusions. In addition, many agencies conduct investigations concerning intrusions into their systems that are not reported to the FBI. In short, this case load represents a large number of incidents.

Several critical elements are required to deal with intrusions into government computer systems. There must be an interagency structure to deal with this problem. No agency should or should have to address these issues alone. Information must be shared with law enforcement and the NIPC. We must work to ensure that any intrusions are stemmed and the vulnerability that allowed the intrusion is patched.

Interagency cooperation is essential in dealing with intrusions into government systems. As I said at the outset, that is why the NIPC was created. Currently the NIPC has representatives from the following agencies at the Center: FBI, Army, Navy, Air Force Office of Special Investigations, Defense Criminal Investigative Service, National Security Agency, United States Postal Service, Department of Transportation/Federal Aviation Administration, Central Intelligence Agency, Department of Commerce/Critical Infrastructure Assurance Office, and the Department of Energy. This representation has given us the unprecedented ability to reach back into the parent organizations of our interagency detailees on intrusions and infrastructure protection matters. In addition, we have formed an interagency coordination cell at the Center which holds monthly meetings with U.S. Secret Service, U.S. Customs Service, representatives from DoD investigative agencies, the Offices of Inspector General of NASA, Social security administration, Departments of Energy, State, and Education, and the U.S. Postal Service, to discuss topics of mutual concern.

This representation is not enough, however. The PDD states that,—The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies." The NIPC would like to see all lead agencies represented in the Center. The more broadly representative the NIPC is, the better job it can do in responding to intrusions into government systems.

The NIPC is pursuing three sets of activities that address computer intrusions into government systems: prevention, detection, and response.

PREVENTION:

Our role in preventing cyber intrusions into government systems is not to provide advice on what hardware or software to use or to act as a federal systems administrator. Rather our role is to provide information about threats, ongoing incidents, and exploited vulnerabilities so that government and private sector system administrators can take the appropriate protective measures. The NIPC has a variety of products to inform the private sector and other domestic and international government agencies of the threat, including: alerts, advisories, and assessments; biweekly *CyberNotes*; monthly *Highlights*; and topical electronic reports. These products are designed for tiered distribution to both government and private sector entities consistent with applicable law and the need to protect intelligence sources and methods, and law enforcement investigations. For example, *Highlights* is a monthly publication for sharing analysis and information on critical infrastructure issues. It provides analytical insights into major trends and events affecting the nation's critical infrastructures. It is usually published in an unclassified format and reaches national security and civilian government agency officials as well as infrastructure owners. *CyberNotes* is another NIPC publication designed to provide security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices. It is published twice a month on our website and disseminated in hardcopy to government and private sector audiences.

The NIPC has elements responsible for both analysis and warning. What makes the NIPC unique is that it has access to all-source intelligence from law enforcement, the intelligence community, private sector, international arena, and open sources. No other entity has this range of information. Complete and timely reporting of incidents from private industry and government agencies allows NIPC analysts to make the linkages between government intrusions and private sector activity. We are currently working on an integrated database to allow us to more quickly make the linkages among seemingly disparate intrusions. This database will leverage both the unique information available to the NIPC through FBI investigations and information available from the intelligence community and open sources. Having these analytic functions at the NIPC is a central element of its ability to carry out its preventive mission.

This initiative expands direct contacts with the private sector infrastructure owners and operators and shares information about cyber intrusions and exploited vulnerabilities through the formation of local InfraGard chapters within the jurisdiction of each of the 56 FBI Field Offices. This is critical to infrastructure protection, since private industry owns most of the infrastructures. Further, InfraGard's success belies the notion that private industry will not share information with NIPC or law enforcement. All 56 FBI field offices have InfraGard chapters. There are currently over 900 InfraGard members. The national InfraGard rollout was held on January 5, 2001.

The NIPC is also working with the Information Sharing and Analysis Centers established under the auspices of PDD-63. For example, the North American Electric Reliability Council (NERC) serves as the electric power ISAC. We have developed a program with the NERC to develop an Indications and Warning System for physical and cyber attacks. Under the program, electric utility companies and other power entities transmit incident reports to the NIPC. These reports are analyzed and assessed to determine whether an NIPC alert, advisory, or assessment is warranted to the electric utility community. Electric power participants in the pilot program have stated that the information and analysis provided by the NIPC back to the power companies make this program especially worthwhile. NERC has recently decided to expand this initiative nationwide. This initiative will serve as a good example of government and industry working together to share information and the Electrical Power Indications and Warning System will provide a model for the other critical infrastructures. Eventually the NIPC will need to be able to have a comprehensive nation-wide system for all the infrastructures.

The NIPC is the Sector Lead Agency for the Emergency Law Enforcement Services sector. As part of this mission, the Center has also been asked to by ELES Sector the to have the NIPC Watch and Warning Unit act as the ISAC for the sector. The NIPC is working to implement this request.

DETECTION:

Given the ubiquitous vulnerabilities in existing Commercial Off-the-Shelf (COTS) software, intrusions into critical systems are inevitable for the foreseeable future. Thus detection of these intrusions is critical if the U.S. Government and critical infrastructure owners and operators are going to be able to respond. To improve our detection capabilities, we first need to ensure that we are fully collecting, sharing, and analyzing all extant information from all relevant sources. It is often the case that intrusions can be discerned simply by collecting bits of information from various sources; conversely, if we don't collate these pieces of information for analysis, we might not detect the intrusions at all. Thus the NIPC's role in collecting information from all sources and performing analysis in itself serves the role of detection.

Agency system administrators need to work with FedCIRC and the NIPC. PDD-63 makes clear the importance of such reporting. It states, "All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law." Currently OMB has instructed the agencies that they must report their intrusions to FedCIRC, but reporting to the NIPC is not mentioned. We are working with FedCIRC to define criteria for reporting of incidents to the NIPC for analytical as well as investigative purposes.

In some cases, in response to victims' reports, the NIPC has sponsored the development of tools to detect malicious software code. For example, in December 1999, in anticipation of possible Y2K related malicious conduct, the NIPC posted a detection tool on its web site that allowed systems administrators to detect the presence of certain Distributed Denial of Service (DDoS) tools on their networks. In these cases, hackers plant tools such as Trinoo, Tribal Flood Net (TFN), TFN2K, or Stacheldraht (German for barbed wire) on a number of unwitting victim systems. Then when the hacker sends the command, the victim systems in turn begin sending messages against a target system. The target system is overwhelmed with the traffic and is unable to function. Users trying to access that system are denied its services. The NIPC's detection tools were downloaded thousands of times and have no doubt prevented many DDoS attacks.

The NIPC also led the FBI's multiagency Y2K command center. NIPC personnel were on alert during the rollover period watching for possible malicious activity under the guise of Y2K. NIPC coordinated a nationwide watch effort and distributed reports every four hours round the clock on the situation.

Regarding warning, if we determine that an intrusion is imminent or underway, the NIPC Watch is responsible for formulating assessments, advisories, and alerts, and quickly disseminating them. The substance of those products will come from analytical work done by NIPC analysts. If we determine an attack is underway, we can notify both private sector and government entities using an array of mechanisms so they can take protective steps. In some cases these warning products can prevent a wider attack; in other cases warnings can mitigate an attack already underway. Finally, these notices can prevent attacks from ever happening in the first place. For example, the NIPC released an advisory on March 30, 2001 regarding the "Lion Internet Worm," which is a DDoS tool targeting Unix-based systems. Based on all-source information and analysis, the NIPC alerted systems administrators how to look for this compromise of their system and what specific steps to take to remove the tools if they are found. This alert was issued after consultation with FedCIRC, JTF-CND, a private sector ISAC, and other infrastructure partners.

RESPONSE:

Despite our efforts, we know that government systems will continue to be attacked. Thus we need to determine the origin of these attacks in order to get to the person behind the keyboard for our government to formulate the appropriate response. In the cyber world, determining what is happening is difficult at the early stages. An event could be a system probe to find vulnerabilities or entry points, an intrusion to steal data or plant sniffers or malicious code, an act of teenage vandalism, an attack to disrupt or deny service, or even an act of war. The crime scene itself is totally different from the physical world in that it is dynamic—it grows, con-

tracts, and can change shape. Further, the tools used to perpetrate a major infrastructure attack can be the same ones used for other cyber intrusions (simple hacking, foreign intelligence gathering, organized crime activity to steal property, data, etc. . . .), making identification more difficult. Determining that an event is even occurring thus can often be difficult in the cyber world, and usually a determination cannot be made without a thorough investigation. In the physical world one can see instantly if a building has been bombed or an airliner brought down. In the cyber world, an intrusion may go undetected for some time.

Identification of the perpetrators and their objectives during an event is critical especially in the initial stages. The perpetrators could be criminal hackers, teenagers, electronic protestors, terrorists, or foreign intelligence services. In order to attribute an attack, the NIPC coordinates an investigation that gathers information from within the United Sates using either criminal investigative or foreign counterintelligence authorities, depending on the circumstances. We also rely on the assistance of other nations when appropriate. Obtaining reliable information is necessary not only to identify the perpetrator but also to determine the size and nature of the intrusion: how many systems are affected, what techniques are being used, and what is the purpose of the intrusions—disruption, economic espionage, theft of money, etc. . . .

Relevant information could come from existing criminal investigations or other contacts at the FBI Field Office level. It could come from the U.S. Intelligence Community, other U.S. Government agency information, through private sector contacts, the media, other open sources, or foreign law enforcement contacts. The NIPC's role is to coordinate, collect, analyze, and disseminate this information. Indeed this is one of the principal reasons the NIPC was created.

Because the Internet by its nature embodies a degree of anonymity, our government's proper response to an attack first requires significant investigative steps. Investigators typically need a full range of criminal and/or national security authorities to determine who launched the attack. Under our system the legal authorities for conducting investigations within the United States include: the Computer Fraud and Abuse Act, the Economic Espionage Statute, the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, as well as the relevant executive orders delineating the responsibilities of the intelligence community. Thus the FBI can apply for court orders to get subscriber information from Internet Service Providers, and monitor communications under the Electronic Communications Privacy Act or under the Foreign Intelligence Surveillance Act, depending on the facts of the case as they are known at the time the order is requested. The FBI has designated the NIPC to act as the program manager for all of its computer intrusion investigations, and the NIPC has made enormous strides in developing this critical nationwide program. In that connection, the NIPC works closely with the Criminal Division's Section on Computer Crime and Intellectual Property, the Department's Office of Intelligence Policy and Review, and the U.S. Attorney's Offices in coordinating legal responses.

In the event of a national-level set of intrusions into significant systems, the NIPC will form a Cyber Crisis Action Team (C-CAT) to coordinate response activities and use the facilities of the FBI's Strategic Information and Operations Center (SIOC). The team will have expert investigators, computer scientists, analysts, watch standers, and other U.S. government agency representatives. Part of the U.S. government team might be physically located at FBI Headquarters and part of the team may be just electronically connected. The C-CAT will immediately contact field offices responsible for the jurisdictions where the attacks are occurring and where the attacks may be originating. The C-CAT will continually assess the situation and support/coordinate investigative activities, issue updated warnings, as necessary, to all those affected by or responding to the crisis. The C-CAT will then coordinate the investigative effort to discern the scope of the attack, the technology being used, and the possible source and purpose of the attack.

While we have not seen an example of cyber terrorism directed against U.S. government systems, the NIPC's placement in the FBI's counterterrorism division will allow for a seamless FBI response in the event of a terrorist action that encompasses both cyber and physical attacks. The NIPC and the other elements of the FBI's Counterterrorism Division have conducted joint operations and readiness exercises in the FBI's SIOC. We are prepared to respond if called upon.

Case Examples

Over the past several years we have seen a wide range of cyber threats ranging from defacement of websites by juveniles to sophisticated intrusions sponsored by foreign powers, and everything in between. Some of these are obviously more significant than others. The theft of national security information from a government

agency or the interruption of electrical power to a major metropolitan area would have greater consequences for national security, public safety, and the economy than the defacement of a web-site. But even the less serious categories have real consequences and, ultimately, can undermine confidence in e-commerce and violate privacy or property rights. A web site hack that shuts down an e-commerce site can have disastrous consequences for a business. An intrusion that results in the theft of credit card numbers from an online vendor can result in significant financial loss and, more broadly, reduce consumers' willingness to engage in e-commerce. Because of these implications, it is critical that we have in place the programs and resources to investigate and, ultimately, to deter these sorts of crimes.

In addition, because it is often difficult to determine whether an intrusion or denial of service attack, for instance, is the work of an individual with criminal motives or foreign nation state, we must treat each case as potentially serious until we gather sufficient information to determine the nature, purpose, scope, and perpetrator of the attack. While we cannot discuss ongoing investigations, we can discuss closed cases that involve FBI and other agency investigations in which the intruder's methods and motivation were similar to what we are currently seeing. A few illustrative are described below:

In hacker cases, the attacker's motivation is just to see how far he can intrude into a system. This seems to be the motivation for the California teens in the well-known Solar Sunrise case. In this case the intruders exploited a well known vulnerability in computers that run on the Sun Solaris operating system. By exploiting this vulnerability, the intruder can gain root access (total control) of the system. As in the Solar Sunrise case, the intruders can then install their own accounts on the system and create backdoors into the system from which they can then install additional programs to find passwords. They also had the ability to alter, remove, or destroy data on those systems. This case demonstrated to the interagency community how difficult it is to identify an intruder until all of the facts are gathered through an investigation, and why assumptions cannot be made until sufficient facts are available. The incident also vividly demonstrated the vulnerabilities that exist in our networks; if these individuals were able to assume "root access" to certain unclassified DoD systems, it is not difficult to imagine what hostile adversaries with greater skills and resources would be able to do. Finally, Solar Sunrise demonstrated the need for interagency coordination to deal with such attacks. The perpetrators in this case were two 16 and an 18 years old.

We have also seen cases of hacking and mischief for what might be termed personal reasons. For example, Eric Burns, a.k.a Zyklon, hacked into the White House web site as well as other sites. This case was worked jointly by the U.S. Secret Service and the FBI. He was caught and pled guilty to one count of 18 U.S.C.1030. In November 1999 he was sentenced to 15 months in prison, 3 years supervised release, and ordered to pay $36,240 in restitution and a $100 fine.

In another example, the Melissa Macro Virus was reportedly named after an exotic dancer from Florida; this virus wreaked havoc on government and private sector networks in March 1999. He pled guilty to one federal count of violating 18 U.S.C. 1030 and four state counts. He admitted to causing $80 million in damage as well. David Smith, the author of the virus, faces a maximum sentence of five years and $250,000 on the federal charge. He is currently awaiting sentencing. This is a good example of how federal and state governments are increasingly coordinating investigations and prosecutions in combating computer crime.

In another case, system penetration coupled with theft can be the motivation. A Florida youth admitted to breaking into 13 computers at the Marshall Space Flight Center in Huntsville, Alabama in June 1999 and downloading $1.7 million in NASA proprietary software that supports the International Space Station's environmental systems. NASA has estimated the cost to repair the damage at $41,000. The subject has also admitted to entering Defense Department systems of the Defense Threat Reduction Agency, intercepting 3,300 e-mail messages, and stealing passwords from Pentagon computers. This case was investigated by NASA. He was sentenced to six months in a juvenile detention center for hacking into NASA computers which support the International Space Station.

Virus writers have become a more prevalent threat in recent years. We have seen virus writers unleash havoc on the Internet for a variety of motivations. In May 2000 companies and individuals around the world were stricken by the "Love Bug," a virus (or, technically, a "worm") that traveled as an attachment to an e-mail message and propagated itself extremely rapidly through the address books of Microsoft Outlook users. The virus/worm also reportedly penetrated at least 14 federal agenciesCincluding the Department of Defense (DOD), the Social Security Administration, the Central Intelligence Agency, the Immigration and Naturalization Service, the Department of Energy, the Department of Agriculture, the Department of

Education, the National Aeronautics and Space Administration (NASA), along with the House and Senate.

Investigative work by the FBI's New York Field Office, with assistance from the NIPC, traced the source of the virus to the Philippines within 24 hours. The FBI then worked, through the FBI Legal Attaché in Manila, with the Philippines' National Bureau of Investigation, to identify the perpetrator. The speed with which the virus was traced back to its source is unprecedented. The prosecution in the Philippines was hampered by the lack of a specific computer crime statute. Nevertheless, Onel de Guzman was charged on June 29, 2000 with fraud, theft, malicious mischief, and violation of the Devices Regulation Act. However, those charges were dropped in August by Philippine judicial authorities. As a postscript, it is important to note that the Philippines' government on June 14, 2000 reacted quickly and approved the E-Commerce Act, which now specifically criminalizes computer hacking and virus propagation. The Philippine government will not be hindered by insufficient charging authorities should an incident like this one ever occur again. Also, the NIPC continues to work with other nations to provide guidance on the need to update criminal law statutes.

In some cases, we have been able to prevent the release of disastrous viruses against public systems. On March 29, 2000, FBI Houston initiated an investigation when it was discovered that certain small businesses in the Houston area had been targeted by someone who was using their Internet accounts in an unauthorized manner and causing their hard drives to be erased. On March 30, 2000, FBI Houston conducted a search warrant on a residence of an individual who allegedly created a computer "worm" that seeks out computers on the Internet. This "worm" looks for computer networks that have certain sharing capabilities enabled, and uses them for the mass replication of the worm. The worm causes the hard drives of randomly selected computers to be erased. The computers whose hard drives are not erased actively scan the Internet for other computers to infect and force the infected computers to use their modems to dial 911. Because each infected computer can scan approximately 2,550 computers at a time, this worm could have the potential to create a denial of service attack against the E911 system. The NIPC issued a warning to the public through the NIPC webpage, SANS, NLETS, InfraGard, and teletypes to government agencies. On May 15, 2000 Franklin Wayne Adams of Houston was charged by a federal grand jury with knowingly causing the transmission of a program onto the Internet which caused damage to a protected computer system by threatening public health and safety and by causing loss aggregated to at least $5000. Adams was also charged with unauthorized access to electronic or wire communications while those communications were in electronic storage. He faces 5 years in prison and a $250,000 fine.

Revenge by disgruntled employees seems to be another strong motivation for attacks. Insiders do not need a great deal of knowledge about computer intrusions, because their knowledge of victim systems often allows them to gain unrestricted access to cause damage to the system or to steal system data. For example, in July 1997 Shakuntla Devi Singla used her insider knowledge and another employee's password and logon identification to delete data from a U.S. Coast Guard personnel database system. It took 115 agency employees over 1800 hours to recover and reenter the lost data. Ms. Singla was convicted and sentenced to five months in prison, five months home detention, and ordered to pay $35,000 in restitution.

Another case involved a National Library of Medicine (NLM) employee. In January and February 1999 the National Library of Medicine computer system, relied on by hundreds of thousands of doctors and medical professionals from around the world for the latest information on diseases, treatments, drugs, and dosage units, suffered a series of intrusions where system administrator passwords were obtained and hundreds of files downloaded, including sensitive medical "alert" files and programming files that kept the system running properly. The intrusions were a significant threat to public safety and resulted in a monetary loss in excess of $25,000. FBI investigation identified the intruder as Montgomery Johns Gray, III, a former computer programmer for NLM, whose access to the computer system had been revoked. Gray was able to access the system through a "backdoor" he had created in the programming code. Due to the threat to public safety, a search warrant was executed for Gray's computers and Gray was arrested by the FBI within a few days of the intrusions. Subsequent examination of the seized computers disclosed evidence of the intrusion as well as images of child pornography. Gray was convicted by a jury in December 1999 on three counts for violation of 18 U.S.C. 1030. Subsequently, Gray pleaded guilty to receiving obscene images through the Internet, in violation of 47 U.S.C. 223. Montgomery Johns Gray III was sentenced to 5 months prison, 5 months halfway house, 3 years probation and ordered to pay $10,000 in restitution and assessments.

We are also seeing the increased use of cyber intrusions by criminal groups who attack systems for purposes of monetary gain. In September, 1999, two members of a group dubbed the "Phonemasters" were sentenced after their conviction for theft and possession of unauthorized access devices (18 USC § 1029) and unauthorized access to a federal interest computer (18 USC § 1030). The "Phonemasters" were an international group of criminals who penetrated the computer systems of MCI, Sprint, AT&T, Equifax, and even the National Crime Information Center. The Phonemasters' methods included "dumpster diving" to gather old phone books and technical manuals for systems. They used this information to trick employees into giving up their logon and password information. The group then used this information to break into victim systems. One member of this group, Mr. Calvin Cantrell, downloaded thousands of Sprint calling card numbers, which he sold to a Canadian individual, who passed them on to someone in Ohio. These numbers made their way to an individual in Switzerland and eventually ended up in the hands of organized crime groups in Italy. Cantrell was sentenced to two years as a result of his guilty plea, while one of his associates, Cory Lindsay, was sentenced to 41 months.

Terrorists groups are increasingly using new information technology and the Internet to formulate plans, raise funds, spread propaganda, and to communicate securely. In his statement on the worldwide threat in 2000, Director of Central Intelligence George Tenet testified that terrorists groups, "including Hizbollah, HAMAS, the Abu Nidal organization, and Bin Laden's al Qa'ida organization are using computerized files, e-mail, and encryption to support their operations." In one example, convicted terrorist Ramzi Yousef, the mastermind of the World Trade Center bombing, stored detailed plans to destroy United States airliners on encrypted files on his laptop computer. While we have not yet seen these groups employ cyber tools as a *weapon* to use against critical infrastructures, their reliance on information technology and acquisition of computer expertise are clear warning signs. Moreover, we have seen other terrorist groups, such as the Internet Black Tigers (who are reportedly affiliated with the Tamil Tigers), engage in attacks on foreign government web-sites and email servers. During the riots on the West Bank in the fall of 2000, Israeli government sites were subjected to e-mail flooding and "ping" attacks. The attacks allegedly originated with Islamic elements trying to inundate the systems with email messages. As one can see from these examples overseas, "cyber terrorism"—meaning the use of cyber tools to shut down critical national infrastructures (such as energy, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population—is thus a very real threat.

We have worked closely with our international partners on computer intrusion cases, including cases in which hackers have illegally accessed U.S. government systems. In 1999 the FBI cooperated with New Scotland Yard in the United Kingdom on a case in which a UK citizen confessed to breaking into U.S. Navy systems. He was further suspected of intruding into other systems, including that of the U.S. Senate. He was sentenced to a term of 3 years on a probation-like status.

We believe that foreign intelligence services have adapted to using cyber tools as part of their information gathering tradecraft. While I cannot go into specific cases, there are overseas probes against U.S. government systems every day. It would be naïve to ignore the possibilty or even probability that foreign powers were behind some or all of these probes. The motivation of such intelligence gathering is obvious. By combining law enforcement and intelligence community assets and authorities under one Center, the NIPC can work with other agencies of the U.S. government to detect these foreign intrusion attempts.

The prospect of "information warfare" by foreign militaries against our critical infrastructures is perhaps the greatest potential cyber threat to our national security. We know that many foreign nations are developing information warfare doctrine, programs, and capabilities for use against the United States or other nations. Knowing that they cannot match our military might with conventional or "kinetic" weapons, nations see cyber attacks on our critical infrastructures or military operations as a way to hit what they perceive as America's Achilles heel B our growing dependence on information technology in government and commercial operations. For example, two Chinese military officers recently published a book that called for the use of unconventional measures, including the propagation of computer viruses, to counterbalance the military power of the United States.

CONCLUSION

While the NIPC has accomplished much over the last three years in building the first nationallevel operational capability to respond to cyber intrusions, much work remains. We have learned from cases that successful network investigation is highly

dependent on expert investigators and analysts, with state-of-the-art equipment and training. We have built that capability both in the FBI Field Offices and at NIPC Headquarters, but we have much work ahead if we are to build our resources and capability to keep pace with the changing technology and growing threat environment, while at the same time being able to respond to several major incidents at once.

We are building the international, agency to agency, government to private sector, and law enforcement partnerships that are vital to this effort. The NIPC is well suited to foster these partnerships since it has analysis, information sharing, outreach, and investigative missions. We are working with the executives in the infrastructure protection community with the goal of fostering the development of safe and secure networks for our critical infrastructures. While this is a daunting task, we are making progress.

Within the federal sector, we have seen how much can be accomplished when agencies work together, share information, and coordinate their activities as much as legally permissible. But on this score, too, more can be done to achieve the interagency and publicprivate partnerships called for by PDD63. We need to ensure that all relevant agencies are sharing information about threats and incidents with the NIPC and devoting personnel and other resources to the Center so that we can continue to build a truly interagency, "national" center. Finally, we must work with Congress to make sure that policy makers understand the threats we face in the Information Age and what measures are necessary to secure our Nation against them. I look forward to working with the Members and Staff of this Committee to address these vitally important issues.

Thank you.

Mr. GREENWOOD. We thank you for your testimony.

Mr. Noonan.

TESTIMONY OF TOM NOONAN

Mr. NOONAN. Mr. Chairman, thank you for having me today, and other members of the committee. I am very pleased to be here to talk about an issue that we are both passionate about, and an issue of, I believe, very critical national security.

Although the folks from the DOE are not here, I thank them because I recognize some of the technology that we pioneered about 8 years ago, and they are using it today effectively to protect the DOE, as are other government agencies, and I am always pleased to see our technology in use.

I am here today to provide you with some background information on threat assessment, on the vulnerabilities and threats that we see in the commercial sector, on the vulnerabilities and threats that we see in working with some 26 foreign governments outside of the United States as well as some 9,000 commercial customers around the globe.

Every day we get involved in one side or the other of hacking, either protecting networks from hackers, cyber thieves and others; or addressing vulnerabilities, fixing the weaknesses necessary to protect those systems. These individuals typically use the Internet to address their own pursuits, including international cyberterrorism, causing havoc and mayhem. I am far less concerned about teenage hackers, although they seem to make the press more often, and become far more concerned with the sophisticated attacks against not just our government but our industry.

As a company, we monitor and manage the security of companies around the world through security operations centers we have located in Sweden, the U.S., Japan, the Philippines, Italy, Rio de Janeiro, and Atlanta, Georgia. So we have an interconnected network of security operation centers monitoring companies and detecting and tracking threats around the world.

Over the years, I have watched computer vulnerabilities increase dramatically. The Internet is so useful for the reasons that it is so vulnerable. I would like to share two analogies. The first analogy I would like to use is to compare a computer to that of a house. Most of you are familiar with your house. You typically have a front door, a back door, and some windows that periodically you lock or monitor through your system. Every single computer connected to the Internet has the equivalent of 65,536 doors and windows, and many of them cannot be locked. They cannot be locked because you are using those doors and windows for legitimate access. So the real challenge becomes, with all of these doors and windows, how do we ultimately determine which need to be locked and which need to be left open, and those that are left open, how are they monitored to assure proper use and access of the system?

If you multiply 65,000 times all of the computers on the Internet, that is how many potential ways to access computers there are. It is simply not a problem that we can address manually. We have to use technology and automation as part of that solution.

So just as physical security companies like ADT or Honeywell or Brinks monitor physical locations, security companies, ours being one of them, have not only pioneered the technology to provide this monitoring—some of the tools you saw from the DOE, for instance—but also to deliver that as a service. I think that is an area that government ought to responsibly look at as we move forward: the area of managed security systems.

My second analogy compares computer security to a chess game. In a chess game, the goal is to protect the king. In information security, the goal is to protect information but otherwise provide legitimate access to it for nonmalicious purposes. But a knowledgeable chess player is required to maneuver and play the chess game, just like a knowledgeable security person is required to help coordinate and manage the overall security posture of a system.

I think we are fooling ourselves if we think that every single user of every computer is going to be aware enough to check their own systems for back doors, to deal with the problems that are so deeply routed in the technology underneath this. Just as a chess game environment is constantly changing, so is the network. New applications, new users, new trading partners, new introductions of sensitive data, et cetera. Over the years, as the Internet has become more used in business and more acceptable to the masses, it has been attacked at an increasing rate.

Incidents occur when hackers maneuver through a system, take advantage of the vulnerabilities and cause a system breach.

So as to your question, Mr. Chairman, there is a whole new currency on the Internet, it is called the back door. Today I could easily trade two DOTs for one GM or a Procter & Gamble for another back door in some other case. So on the Internet, back doors or accounts are being used as a new currency, and they are being traded frequently.

Vulnerabilities are holes or weaknesses and problems that exist in the computer systems, as we saw from the DOE demonstration, and these incidents include everything from credit card theft, which seems to be where the consumers' fear is, to the compromise of very sensitive systems. And it comes down to three things:

One, confidentiality. Is and can the information be protected?

Two, integrity. Can it be changed to questions that came from the Chair?

And, last, is it available? Denial of service, which you have heard, the ability to completely shut down or destroy data is possible here.

So what I would like to do is introduce three slides to demonstrate what is happening in industry. The first slide demonstrates top security breaches. As you can see, 4 percent of the breaches are actually physical security breaches such as breaking into a window or getting through a locked door.

Let us look beyond that into where the real computer security problems are. Twenty percent are system unavailability breaches or denial of service breaches. We learned about those in February of last year when some of the most important commerce sites on the Internet were taken off line by malicious activity.

Also, as Mr. Dick has commented on, the "ILUVYOU" e-mail virus cost industry billions of dollars. Electronic exploits represent about 20 percent of the breaches. An example of an electronic exploit is finding a hole and installing a back door. The gentleman from the DOE showed you how easy that is. Last, 25 percent of the breaches are loss of privacy or confidentiality breaches such as when someone compromises a record or data base and removes information. Twenty-six percent are malicious code breaches, things like when a hacker sends an attachment with a malicious payload and, when opened, it deletes files automatically.

To give you an idea how fast incidents are occurring, the second slide examines the increase in one type of breach: the virus. If you look at the threat spectrum, on one side you have the traditional virus all of the way up through denial of service attacks, trojans, worms, electronic compromise of data bases and operating systems.

But if you look at this slide, you can see that viruses in October 1999 alone, there were more than 2,000 new known viruses. In November 1999, there were over 2,400. In December 1999, over 2,500 more were added. In October 2000, there were 30,678 new viruses being tracked; and in November of 2000, there were some 23,962 new viruses. What we are seeing here is exponential growth of an issue that is getting out of hand and causing significant damage and problems to the global computing infrastructure.

I would like to give you a better idea of how incidents generally occur and how computer security companies protect against these incidents.

The third slide is an example of a Website where crackers can get information to help them break into a system. This is a Website that I have deattributed. Being in the protection business, I don't like to pass along where people can go get these weapons. This actually came from an African hacking site, and in this hacking site it is basically the equivalent of being able to anonymously walk down to your corner store, pick up an anthrax bomb and a couple of grenades, and be able to launch them from your own computer anonymously and without any visibility as to who you are. These happen to be computer exploits.

You can take back doors that monitor and take advantage of microphones, denial of service attacks, you have a whole smorgasbord up here to fill your palate.

This site lists new vulnerabilities that have been discovered and programs that allow anyone to use these exploits to damage a system. There are literally thousands of these sites on the Internet, so you do not have to be very sophisticated or have a high IQ to cause a lot of damage to our infrastructure.

We monitor the Websites that discover the latest trends. In addition, thousands of private chat rooms exist where more sophisticated crackers trade hacking tools over the Internet.

We are pleased that the government is interested in taking computer security seriously. The United States spends billions of dollars buying weapons and gaining intelligence to protect our country. Our computer systems must be adequately protected or our entire infrastructure could be compromised by one single person with one single computer.

Even though the task is complicated, computer systems can be protected. I think today we focused on how easy they are to break in. I think it might be helpful someday to have a session on how effectively we can protect the computer systems today because this is where we are going to take action. I think the government has taken great strides in the past few years, but much more is needed. I think we are moving from the topical to the awareness to let us start taking some action here.

As industry has considerable resources and expertise, a continued partnership with industry is crucial. In addition, computer systems should be a priority, and leadership and coordination are necessary in the government. The government has done well with the resources it has been given. However, computer security specialists we believe are required to implement and coordinate many different security products and services to adequately secure a system.

In my company alone, the average salary of one of my 2,000 employees is around $80,000. I don't know of an industry where the average employee from the mailman to the CEO is $80,000. Computer security experts are scarce. They are in short supply and they are expensive. To help address the cost of computer security, I think we ought to focus not just on what do we do to protect our infrastructure, but we ought to extend these efforts to educational efforts that we can undertake to train the personnel coming out of our schools, not just our engineering schools, but our colleges and universities. Computer programmers should be trained in computer security. Today they are not. Today they are trained in how do you make the best feature. What they do not focus on is the vulnerability that they leave behind.

Specialized programs in computer security should be encouraged, and we are strongly supportive of the universities that are implementing them today. I look forward to a continuing dialog on computer security issues. Working together, we are confident we can adequately secure our country's assets and information. Thank you.

[The prepared statement of Tom Noonan follows:]

PREPARED STATEMENT OF TOM NOONAN, PRESIDENT AND CEO, INTERNET SECURITY SYSTEMSGOOD MORNING, MR. CHAIRMAN AND MEMBERS OF THE COMMITTEE. I AM PLEASED TO APPEAR BEFORE YOU TODAY TO DISCUSS AN ISSUE OF GREAT IMPORTANCE TO OUR COUNTRY.

BACKGROUND

In 1991, the founder and Chief Technology Officer of Internet Security Systems, Chris Klaus, became interested in government security while interning at the Department of Energy. Chris then began working on a groundbreaking technology that actively identified and fixed computer security weaknesses. The next year, while attending Georgia Institute of Technology ("Georgia Tech"), Chris released his product for free on the Internet. He received thousands of requests for his invention, and decided that he should sell it. In 1994, I met Chris over the Internet and teamed with him to form Internet Security Systems. I was then working for a computer company, having attended GA Tech and Harvard Business School. Chris and I then launched the company's first product, Internet Scanner, and went public in March 1998. And yes, we're a profitable company, even in today's market. Today, Internet Security Systems is the worldwide leader in security management software. For nearly 10 years, which is several lifetimes in Internet time, we have been involved in computer security, watching the area grow from the outset. Chris Klaus (who is now 26) is one of a handful of premiere experts in the world on computer security, and Internet Security Systems is a widely recognized pioneer in computer security. Computer security is all we do. We have nearly 2,000 employees in 18 countries focused exclusively on computer security. Altogether, we now have more than 8,000 customers, including 68 percent of the Fortune 500, and 21 of the 25 largest U.S. commercial banks. We also serve the ten largest telecommunication companies, numerous U.S. government agencies, and other non-U.S. governments.

VULNERABILITIES

I'm here today to provide you with some background information on threat assessment. Every day, Internet Security Systems stops criminal hackers and cyber-thieves by addressing vulnerabilities in computers. The individuals who use the Internet for business to business warfare, for international cyber-terrorism, or to cause havoc and mayhem in our technology infrastructure. Internet Security Systems is involved in every aspect of computer security, whether in making the security products or in managing them. We also monitor networks and systems around the clock (24 x 7 x 365) from the US, Japan, South America, and Europe in our Security Operations Centers ("SOCs"). We search for attacks and misuse, identify and prioritize security risks, and generate reports explaining the security risks and what can be done to fix them. At the heart of our solution is our team of world-class security experts focused on uncovering and protecting against the latest threats. This team of 200 global specialists, dubbed the X-Force, understands exactly how to transform the complex technical challenges into an effective, practical, and affordable strategy. Because of all of these capabilities, companies and governments turn to us as their trusted computer security advisor.

Over the years, I have watched computer vulnerabilities increase dramatically. The Internet is so useful for the very reasons that it is so vulnerable. To give you an idea of what we are dealing with, I'd like to share two analogies. First, I'll compare a computer to a house. Every computer connected to the Internet has the equivalent of 65,536 doors and windows which need to be locked and monitored to make sure no one breaks in. Multiply 65,536 by every computer in every company and you begin to see the extent of the problem. Just as physical security companies like ADT monitor your physical doors and windows, computer security companies must lock and monitor the doors and windows of computers.

My second analogy compares this complicated area of computer security to a Chess game. In a Chess game, the goal is to protect the king—or mission critical information. The other Chess pieces protect the king. But a knowledgeable Chess player is required to maneuver the Chess pieces. With computer security, the goal is to protect the information. A variety of computer security products, including Intrusion Detection Systems (IDS) and vulnerability assessment, function as Chess pieces, and protect and watch the information. These products are absolutely essential. However, you also need to have a computer security expert to manage these products, just as you have to have a knowledgeable Chess player maneuver the Chess pieces. Just as a Chess game environment is constantly changing, the computer security environment is also constantly changing. Computer security companies, such as Internet Security Systems, produce the products and perform the serv-

ices that protect the information and manage the products so that they function in the proper way.

Over the years, as the Internet has become more used in business and more accessible to the masses, it has been attacked at an increasing rate. Incidents occur when hackers maneuver through a system, take advantage of the vulnerabilities, and cause a system breach. Vulnerabilities are holes, weaknesses, and problems that exist in computer systems. Incidents include credit card theft or other information theft. The first slide documents the top security breaches. 4% of these breaches are actual physical security breaches, such as breaking a window or getting in through a locked door. 20% are system unavailability breaches or denial-of-service breaches, such as the "ILUVYOU" email virus. Electronic exploits represent 20% of the breaches. An example of an electronic exploit is finding a hole where you can install a backdoor to get into a computer system. 25% of the breaches are loss of privacy or confidentiality breaches, such as when a cracker breaks into a database server and gains access to credit card information. 26% are malicious code breaches, such as when a hacker sends an email with an attachment that when opened, deletes files on the computer system. 5% of the breaches are other breaches.

To give you an idea of how fast incidents are occurring, the second slide examines the increase in just one type of breach, the virus. Viruses, such as the "ILUVYOU" virus are mini computer programs that flood a computer system with email so that the system slows down or crashes. Viruses can also destroy information on a computer system. In October 1999 alone there were more than 2000 new known viruses. In November 1999, there were 2,427 new viruses. In December 1999, 2,586 were added. Look at how these numbers have dramatically increased in 2000. In October 2000, there were 30,678 new viruses. In November 2000, there were 23,962 new viruses. In December 2000, there were 16,762 new viruses. Keep in mind that the vast impact caused by the "ILUVYOU" virus was caused by only one of these viruses.

To give you a better idea of how incidents generally occur, and how computer security companies protect against these incidents, the third slide is an example of a Web site where crackers can get information that will help them break into a system. Because we are in the protection business, we have modified this site and removed the identifying information. This site lists new vulnerabilities that have been discovered, and includes programs that allow anyone to use these to exploit vulnerabilities to damage a system. There are thousands of similar Web sites. Our X-Force monitors the most important Web sites to discover the latest trends. In addition, thousands of private chat rooms exist where more sophisticated crackers trade hacking tools over the Internet. Our X-Force gains access to important chat rooms and monitors them as well.

RECOMMENDATIONS

We are pleased that the Government is interested in taking computer security seriously. The United States spends billions of dollars buying weapons and gaining intelligence to protect our country from more conventional types of attack. Our computer systems must also be adequately protected, or our entire infrastructure could be compromised by one person with one computer. Even though the task is complicated, computer systems can be protected.

The Government has taken great strides in the past few years. However, much, much more is needed. As industry has considerable resources and expertise, a continued partnership with industry is crucial. In addition, computer security must be a priority, and leadership and coordination are necessary in the Government. International leadership is also required. Perhaps most importantly, funding for secure Government systems must be increased by a substantial amount, and outsourcing should be considered as an option. The Government often does well with the resources it has been given. However, computer security specialists are required to implement and coordinate many different security products and services to adequately secure a system. As computer security expertise is extremely rare, the cost of computer security specialists is astronomical. In my company alone, the average salary of my 2000 employees is around $80,000. To help address the cost of computer security, educational efforts must be undertaken to train the personnel required. Computer programmers in universities should be trained in computer security. Currently, they are not. In addition, specialized programs in computer security should be encouraged.

Thank you for inviting me here today. I look forward to a continuing dialog on the computer security issue, and hope that, working together, we can adequately secure our country's assets and information.

Mr. GREENWOOD. Thank you very much for your extraordinary testimony.

The Chair recognizes himself for 5 minutes for questions.

Ms. McDonald, on your chart, the route compromises, 155 last year, are those the kind of compromises that we saw in the demonstration where you can essentially take over an entire system?

Ms. MCDONALD. Yes.

Mr. GREENWOOD. Question for Mr. Dick. You referred to the issue of who is sitting behind the keyboard. Can you elaborate on what the FBI has discovered as to who these perpetrators are? We know that there are teenagers who will hack into systems for the fun of it. But in terms of identified perpetrators, can you share with us what their motivations have been?

Mr. DICK. In the physical world, the range and motives associated with who are perpetrating these kinds of acts runs the full gamut. As Tom was referring to, we have the teenage hackers that are doing it for sport and notoriety on the Internet, to the other range where we have state-sponsored activities associated with trying to discern how to conduct information warfare.

What we see in the range of what we refer to as southern vulnerabilities, you have a high volume of, let us say, the hackers that are going into systems for the honor or recognition of it—which is relatively low impact as far as our national security and economic well-being—which is going down the virus writers, which does have an economic impact on us, to criminal organizations. We are now seeing both U.S. and foreign criminal organizations attacking systems for credit card information, and then going back and extorting the businesses out of funds for not recognizing or exposing that they have been vulnerable to espionage and so forth.

Mr. GREENWOOD. What are the kind of penalties that have been exacted against these perpetrators, and do you believe the penalties are adequate under the current Federal statutes?

Mr. DICK. For violations of Title 18, section 1030, the penalties are 10 years in jail for each violation. The maximum penalties associated probably are adequate.

Now, have the courts, based upon the sentencing guidelines, levied those kinds of penalties to subjects which have been convicted? Not at this point. It is very similar to white collar crime investigations where the penalties are perceived by some to be less than adequate. But I think with time, that will change also.

Mr. GREENWOOD. What about international cooperation? You referenced the case in the Philippines where they were not—their laws did not permit us to prosecute that perpetrator. Are there in process efforts to create international agreements or treaties with regard to these hackers?

Mr. DICK. Yes. There are a number of things ongoing right now through the G-8 and the Council of Europe to implement laws that will more standardize not only our ability to prosecute, but our ability to access information.

One of the difficulties in investigating these cases is almost 99 percent of the time, we are going to end up overseas in some faction of the case because of particular hot point or place that they intruded into overseas to get into the U.S. system exists. So we have to go to a foreign entity just to get the information as to what

occurred over there. There are efforts going on and more could be done. There is a lot of emphasis on that at this point in time.

Mr. GREENWOOD. Thank you.

Mr. Noonan, I think you made some reference in your testimony to Federal customers that you have, U.S. Government customers.

Mr. NOONAN. Yes.

Mr. GREENWOOD. Do they tend to be the inspectors general buying your services and software so they can check on the departments, or do they tend to be the managers of those departments buying your software so as to provide the protections necessary?

Mr. NOONAN. Historically they have been more the watchdog or audit, inspector general type function, meaning using the technology to determine where the systems are vulnerable.

Today we are beginning, and just beginning to see the beginnings of more widespread use in intrusion detection. Vulnerability detection and intrusion detection are kind of the yin and yang. One finds the holes, and the other watches to make sure that the other does not exploit the holes.

Operationally, you want to see the units, using both vulnerability detection to fortify the environment and intrusion detection to monitor it to ensure that it is being used judiciously.

Historically it has been mainly the watchdog part. That is just now beginning to turn to more operational use.

Mr. GREENWOOD. Do you and your competitors aggressively market your services to the systems managers within the Federal Government? Do you have conferences and exhibits and so forth where these Federal managers can come and survey this technology?

Mr. NOONAN. Yes, we do, as do many in the industry. One thing that is of particular note is movement in this area has really just begun in the last 6 to 9 months in terms of active technologies that can be deployed to protect the infrastructure. If I had to take a guess, I would probably say that 5 percent, maybe, of the government actually is protected with these types of technologies operationally. And I could be off by as much as 5 percent. Regardless, I think we have a long way to go.

Ms. MCDONALD. Mr. Chairman, one of the things that we are doing in FedCIRC this fiscal year is evolving into an intrusion detection system that is called Managed Security Services, much like what Mr. Noonan's company offers.

We are encouraging Federal agencies to deploy managed security services; and hopefully we are responsible for maybe some of that 5 percent, if 5 percent exists. It is our intention in the FedCIRC organization to, after we have encouraged agencies to implement managed security services and intrusion detection systems, that we will develop an analysis capability within FedCIRC so that these intrusion detection systems will feed up into the FedCIRC program office and we will be able to get a picture, a much better picture across government as to what is actually occurring.

With this step we feel that we can move from the 20 percent of the incidents that are being discovered to closer to the 100 percent.

Mr. GREENWOOD. Mr. Noonan, since the bad guys can use your services or at least your software, do you have any process of screening out the bad guys?

Mr. NOONAN. Mr. Chairman, it would be very difficult for the bad guys to use our technology. Each is encrypted with a special key. Each user that licenses the software is required to provide information and sign a license agreement. So our systems are not freely available, and they do not operate unless you have a key generated by us, and each key is specific to that user.

So if the DOE licensed our vulnerability system, they could not use it on the Department of Transportation computers because it would not match up with their IP addresses.

Mr. GREENWOOD. The Chair recognizes the gentleman, Mr. Strickland.

Mr. STRICKLAND. Ms. McDonald, I have a copy here of a March 2001 newsletter from FedCIRC about the demise of the FedNet, which has been described as a conceptualized weapon to defend the Federal information infrastructure by tracking anomalous behavior. According to this newsletter, FedNet was buried because of concerns of the public, media, and Congress because it was a threat to privacy rights. Are you familiar with this?

Ms. MCDONALD. I am familiar with that, sir. If I could explain——

Mr. STRICKLAND. If you could explain to me what you do not agree with.

Ms. MCDONALD. We did not bury FedNet. FedNet first came to the public's attention in a New York Times article in 1998. That article said that FedNet was a system that was going to be run by the FBI, and that it was going to monitor all citizens' e-mails, including the content of those e-mails, in the United States. FedNet was actually a program the GSA was sponsoring, not the FBI, and the idea was to develop an intrusion detection network with all of the Federal civilian agencies.

Because of the bad publicity that it got, we revamped the program. We now call it the managed security services, which is what I alluded to. And what we have done, so that agencies have confidence in what we are doing in the FedCIRC program, is we are encouraging agencies to establish intrusion detection systems within their own organizations and then work with FedCIRC on a voluntary basis.

One of the important facts of this entire area is trust. We lost a lot of trust with the FedNet program, which is why we chose to rename it managed security services. And as the industry has matured, and as Mr. Noonan has testified, these services are commercially available and we are encouraging agencies to procure these services themselves and then work with FedCIRC.

Mr. STRICKLAND. Ms. McDonald, this is your publication?

Ms. MCDONALD. That's correct.

Mr. STRICKLAND. It indicates that Federal civilian agencies for questionable activities, to provide those same agencies a vehicle to obtain those services from private industry. I think we are talking about the services that were envisioned in FedNet. FedCIRC is preparing a new offering that would employ private industry and will consist of a variety of information security services under the caveat managed security services.

Now, is this an attempt by the GSA to go—to sneak around behind the back of Congress and set up, if not the same system, cer-

tainly a similar system, as a way of avoiding the kind of criticism that was directed toward the previous effort?

Ms. MCDONALD. Absolutely not. The idea was to make it much more palatable to the Federal civilian agencies, to put them in control of the systems because they would be the ones that would be procuring what is now a commercially available service. FedNet as it was designed or thought of in 1998 didn't really exist. But that shows the maturity in this entire field. Now these services are available commercially, and it is important for agencies to trust the FedCIRC operation. So we are encouraging them to deploy these services and then share the results of those systems with us.

Mr. STRICKLAND. Yes. If you can just speak to this question. Under the services available from the managed security services program, will the public be able to have confidence that all of their communications will not be tracked or trackable?

Ms. MCDONALD. Absolutely.

Mr. STRICKLAND. That is still a concern?

Ms. MCDONALD. That was a misunderstanding from the New York Times article. These systems are going to be deployed only at Federal agencies looking at Federal agency systems, and they will not be looking at the content of those systems.

Mr. STRICKLAND. So you are saying to me, if a private citizen attempts or does gather information from some Federal source, some Federal agency, that it will not be possible to track that communication to identify it?

Ms. MCDONALD. That's correct. Unless that private citizen does something like the Department of Energy demonstrated this morning, it won't show up on an intrusion detection system if it is a normal, approved-type activity.

Mr. STRICKLAND. Reference is made to anomalous behavior. Do you have a definition of what that would be?

Ms. MCDONALD. Behavior that is beyond the normal. For instance, most of us work 9-to-5 jobs. Profiles are developed on a user. If all of a sudden somebody was working at their job at 2 a.m., that would fall into that type of behavior, and that would kick out on the intrusion detection system.

Mr. STRICKLAND. I suspect that a lot of committee and staff members of the House of Representatives would be identified as engaging in anomalous behavior because many of them work at strange hours.

Ms. MCDONALD. That is true. I am sure that if you looked at Mr. Noonan's company's hours, his hours would be quite different than perhaps a Federal agency's hours. But with an intrusion detection system, you profile the culture that occurs in your organization. So perhaps maybe the staffers are not working at 2 o'clock in the afternoon.

Mr. STRICKLAND. It seems to me that the result of this could be, the profiling, a very innocent behavior on the part of American citizens that seem to have work habits that were perceived by someone as anomalous. Is that not something that the American public should have some reasonable concern about?

Ms. MCDONALD. Let me say that this whole area of technology, as you very well know, opens up a tremendous amount of privacy

concerns, and people's activities can be tracked. It is something that we need to balance with the need to protect.

Mr. STRICKLAND. I appreciate the difficulty of the issue that we are discussing today. I think it is important to be open and have full disclosure. I think it is important that the concerns that resulted in the initial action to not proceed be fully explored.

Mr. Chairman, I do think this is a matter that we should continue to follow and to explore as we look more deeply into this.

Ms. MCDONALD. We would be glad to work with you on that. Thank you.

Mr. STRICKLAND. Thank you.

Mr. GREENWOOD. The Chair thanks the gentleman and recognizes the gentlelady from Colorado.

Ms. DEGETTE. Thank you, Mr. Chairman.

We have been hearing a lot of pretty chilling testimony this morning about the risks of this cyberterrorism and other kinds of compromises of our systems.

I am just sitting here wondering—for example, this slide that Mr. Noonan put up with this Website from—not the Website, but this slide from Africa. And I think you said that we wonder if people from places like Africa couldn't hack into our systems and even launch nuclear weapons or biological warfare.

Mr. Dick, in your written testimony you say we have not seen an example of cyberterrorism. With all of this activity going on, I guess I am wondering why we have not seen an example of cyberterrorism yet.

Mr. DICK. In the continuum of incidents and times, over time as people get familiar with the technology, the tools, even get greater availability out on the Internet, you are going to see the volume of activity go up. Eventually we are going to see it.

Ms. DEGETTE. Why do you think that we have not seen it yet?

Mr. NOONAN. I was just going to comment on that. I think we have seen it. We see it in industry. It is just a microcosm. It is not the same necessarily as in the physical world. I have seen entire customer records destroyed. That is terrorism to a business.

Ms. DEGETTE. And that is certainly serious to us. What is your definition of cyberterrorism?

Mr. NOONAN. I think that is a very good question. The tools that I represented—and that is actually a Website which has been copied now and made into a slide. You can click on any one of those and download those weapons, if you will.

My definition of cyberterrorism for a commercial industry is anything that causes significant problems with the availability, the confidentiality, or the integrity of those systems. We can now have very small incidences of cyberterrorism, or very coordinated, large-scale attacks.

Mr. DICK. My definition is different. What he described there, those would be criminal acts that we would investigate under criminal authorities.

When we talk about terrorism in the Department of Justice and from an investigation standpoint, we have governed by certain laws and by who are defined as foreign powers. So my definition is much more restrictive.

Ms. DEGETTE. What is your definition?

Mr. DICK. Basically those foreign powers that are attacking the United States and its assets for political motives as opposed to some sort of economic reason.

Ms. DEGETTE. Why do you think that we have not had any incidence of cyberterrorism on the scale of what Mr. Noonan describes?

Mr. DICK. My statement says we have not had any that we can attribute to any foreign powers, organizations, and acts at this point in time. I am not saying that there never has been.

Ms. DEGETTE. So you think that we might have had cyberterrorism, but we do not know?

Mr. DICK. I have no empirical data that says specifically.

Ms. DEGETTE. First of all, I think we should figure out what our definition of cyberterrorism is. That might be helpful in this analysis. It might be helpful to the public when we think about the safety of our government and Internet systems. I agree with Mr. Strickland that we need a lot more research and hearings on this. But the reason that I am concerned about this issue is because we are here today talking about compromise of government computer systems, and I am trying to figure out what the very real risk is of, say, someone hacking into our military intelligence systems or our defense systems and actually launching these biological weapons or nuclear weapons or obtaining top secret information.

I understand that there are a lot of incidents, but what is the real risk here?

Mr. DICK. When we say, "terrorism," we are looking at things that are politically motivated in an attempt to intimidate our society or policies, or change policies, as opposed to affect a business's way of doing business.

Ms. DEGETTE. Why do you think that we have not had this happen? Do we have pretty good integrity of those critical systems and what we need to do is work on other systems? Ms. McDonald, do you have an opinion on this?

Ms. MCDONALD. I think we are lucky that we have not had it happen.

Ms. DEGETTE. Mr. Noonan, do you have any comments?

Mr. NOONAN. I think we have a lot of problems. I think in terms of the infrastructure, I think that it is very, very widespread; and whether I would comment on whether we have had cyberterrorism or not, I know we have had compromises. I have tracked them and watched them in and out of our own government and agencies.

What networks the Pentagon actually uses to launch nuclear weapons, I don't know. I hope that those are not easily accessible from the Internet. But I know that we have had compromises. Whether we want to call that terrorism or not is up to us.

Ms. DEGETTE. Shifting direction a little bit, Mr. Noonan, these 65,000 doors that you talk about, and computers that allow unauthorized entries, those are part of the operating systems that come with computers when people obtain them?

Mr. NOONAN. That's correct. That is a world standard.

Ms. DEGETTE. Right. I would think that a good portion of the blame for the vulnerabilities in operating systems would lie on the developers of those products; wouldn't you agree?

Mr. NOONAN. Not entirely, but partially, yes; because the Internet standard, PCPIP, which we use all over the world, is open by design, and this is the fundamental challenge.

Ms. DEGETTE. In fact, Microsoft says customers want openness, not closed doors, correct?

Mr. NOONAN. Absolutely. So the conundrum is how do you secure the integrity of the system when it is based on an open design.

Ms. DEGETTE. Do you have any ideas how to do that?

Mr. NOONAN. Absolutely. I absolutely do.

Ms. DEGETTE. Would you share one?

Mr. NOONAN. I believe we are entering an age where everything is going to be microprocessor driven, not just our computers, but the Internet will be the base foundation for command and control systems for distribution tracking systems, for satellite tracking systems, for everything that we do that needs information. The only way that we are going to secure these systems out into the future is if each individual system on the network has its own capability to intelligently monitor itself and discern between good and bad behavior.

Ms. DEGETTE. Thank you. I have one last question, and that is to Ms. McDonald. I assume that is your chart behind you?

Ms. MCDONALD. Yes. It is based upon our data.

Ms. DEGETTE. My question to you is of the route compromises on that chart which are in red, it says a route compromise means that the intruder has gained full administrative or route privileges over the targeted system, meaning that any information or capability of the system is totally owned and is controllable by the intruder.

Ms. MCDONALD. That's correct.

Ms. DEGETTE. How many of those route compromises have been to confidential or secret data?

Ms. MCDONALD. To my knowledge, none.

Ms. DEGETTE. Thank you.

Mr. Chairman, I can see that we have a lot more work to do. I want to thank this excellent panel and the previous one.

Mr. GREENWOOD. The Chair is going to recognize himself for a second round of questions, and I turn to you first, Ms. McDonald.

Of the 586 incidents reported in 2000, is it true that at least several of those are known to have resulted in the compromise of sensitive agency information; and if so, can you give us some sense of the type of information that was compromised?

Ms. MCDONALD. Every Federal civilian agency, as we have heard this morning, maintains very sensitive information on American citizens. I can tell you that most of the increases that we have seen, and most of the incidents in the year 2000 had to do with scientific research and environmentally involved agencies. Again, because this is an area that FedCIRC needs to develop the trust of the agencies that we work with, I could not go into identifying which particular agencies and what systems.

But generally the scientific area is—as Mr. Noonan alluded to, the whole Internet is very open. And it was developed by the scientific area and they, as part of their research, are a very open community.

Mr. GREENWOOD. Your testimony notes there has been a rise in reconnaissance activities, scans of government computers by for-

eign sources over the past year, up from 60 percent in 1999 to 75 percent in 2000. Are we talking about terrorism activities, teenage hackers from abroad, espionage, or a combination of these; and how does FedCIRC determine if a scan is by a foreign source, and what information are these foreign sources trying to gain access to?

Ms. MCDONALD. Well, we can determine whether it's a foreign address where these scans are coming from. If with working with the agency we feel that it is a nation-state then we work with Mr. Dick's area or the NSA and transfer that information over to them. We do not investigate incidents. Our job is to report incidents, assist agencies to recover from incidents, and to give agencies the tools that they need in order to protect themselves.

Mr. GREENWOOD. Mr. Dick, according to a Washington Post article dated March 21 of this year, your current assessment of computer security at Federal facilities is that they are extremely vulnerable to potentially crippling cyberattacks. Is that an accurate assessment of your view; and if so, what is that view based on?

Mr. DICK. It is an accurate assessment of my view of not only government systems but private sector systems as has been demonstrated in this committee today. There are numerous tools out there for which to exploit the vulnerabilities in those systems; and unless there is due diligence on the part of systems administrators, CEOs and executive managements of government agencies, as well as the private sector as a whole, you're going to have vulnerabilities and that includes due diligence not only in the implementation of firewalls and intrusion detection software, but as has been pointed out earlier, continually updating and correcting your systems.

For example, we are conducting an investigation currently, or several investigations, regarding known vulnerabilities to certain operating systems. These intruders are going in, as I alluded to earlier, and taking credit card numbers and then extorting the businesses. In December of this year we issued a warning based upon our investigative efforts to the public saying that these are the known vulnerabilities in this operating system which need to be repaired because of this. We got very little play.

In March we became much more public after coordinating with the information sharing and analysis centers and our other partners and came out with a very—a much more public announcement and beat the drum louder, if you will, to try and get these vulnerabilities fixed because there are known patches that can prevent this. Because of that, one of the information sharing and analysis centers indicated that we were able to prevent over 1,600 attempts.

So the point is that it is continual vigilance and implementation in security; and unless you do that, you are vulnerable.

Mr. GREENWOOD. GSA told this committee—told our staff that in excess of 95 percent of the intrusions into Federal computers could have been prevented had well-known vulnerabilities been patched with existing remedies. What does that say about the state of our computer security and vigilance, Ms. McDonald?

Ms. MCDONALD. It doesn't say a lot.

Mr. GREENWOOD. Actually, it does say a lot.

Ms. MCDONALD. Well, yes it does; but not what I would like to say about it. One of the things that we're doing in the Fed service area, recognizing this being an issue, is working with a number of companies to see what capabilities they have to offer the Federal Government for a patch distribution system so that we can profile the agency systems to determine where—what type systems they have, where they stand on their patches, and then, as patches come out, feed them down to the agencies in a hope that that will encourage them to apply the patches and therefore allow them to recover from——

Mr. GREENWOOD. Well, you're hoping that it will encourage them, but are they required? If you do an advisory indicating a vulnerability in a known patch and you distribute that to the Federal agency, is the Federal agency required——

Ms. MCDONALD. No.

Mr. GREENWOOD. [continuing] under any——

Ms. MCDONALD. No. This would only allow us the knowledge that the patch was delivered to them, and we can establish the system so that we can see if they actually took the patch; but they're under no requirement to apply the patch.

Mr. GREENWOOD. Do you keep records of to what extent your encouragement works in the patches?

Ms. MCDONALD. We will, once we implement the system.

Mr. GREENWOOD. Okay. The Chair thanks all three of our witnesses for their superb testimony and you are excused. And I would call the second panel, consisting of Mr. Robert Dacey, director of information security systems at the U.S. General Accounting Office, and Mr. John S. Tritak, director of Critical Infrastructure Assurance Office of the U.S. Department of Commerce.

I'm going to do what I failed to do in the last panel and that is remind you this committee is holding an investigative hearing and when doing so it has had the practice of taking testimony under oath. Do either of you have any objection to testify under oath?

Mr. DACEY. No.

Mr. TRITAK. Not at all.

Mr. GREENWOOD. You're also then advised that under the rules of the House and under the rules of the committee you're entitled to be advised by counsel. Do you desire to be advised by counsel during your testimony?

Mr. DACEY. I do not.

Mr. TRITAK. I do not.

Mr. GREENWOOD. In that case, will you rise and raise your right hand and I will swear you in.

[Witnesses sworn.]

Thank you. Please be seated.

We will recognize Mr. Dacey for his testimony for 5 minutes.

TESTIMONY OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE; AND JOHN S. TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE, U.S. DEPARTMENT OF COMMERCE

Mr. DACEY. Mr. Chairman, I am pleased to be here this afternoon to discuss information security in the Federal Government. Evaluations by GAO and the Inspectors General continue to show

that computer security over the government's unclassified systems are fraught with serious and widespread weaknesses. The risk associated with these weaknesses as has been discussed earlier are heightened by the increasing interconnectivity of our systems, as well as the use of the Internet. While the government cannot estimate the actual damage and loss, principally because many incidents are either not identified or not reported, I'd like to provide several examples that illustrate the effect that can happen to Federal agencies.

First, there can be theft or misuse of Federal Government resources. For example, one individual embezzled over $435,000 at the Department of Defense. At EPA, a hacker chat room was surreptitiously installed on an agency server. An EPA system was used by hackers to launch attacks against others, and numerous Federal Web sites have been reportedly defaced.

Ineffective security can also result in inappropriate disclosure or misuse of sensitive personal and proprietary business information. For example, sensitive information was reported stolen by the Department of Defense. IRS employees have browsed taxpayer records and used information obtained to commit financial and other crimes. Social security information has been sold to facilitate identity theft.

Another effect is potential disruption of business operations. For example, operations at several agencies were disrupted by the "I love you" virus. Also, users were locked out of EPA systems using some of the techniques we saw demonstrated earlier today.

And third, DOE stood down its Internet connections on several occasions. The last can result in modification or destruction of programs or data. For example, sensitive information was corrupted and malicious software installed at the Department of Defense.

While agencies' operations and risks vary, the types of weaknesses reported are strikingly similar. In general, systems did not have adequate controls to prevent and detect unauthorized changes to systems software, to prevent or detect unauthorized access to facilities, systems, programs and data, and to ensure the continuity of business operations.

We and the Inspectors General made scores of recommendations to improve security, and in 2001 we again reported information security as a high-risk area, as we have in 1997 and 1999.

I would like to point out that GAO employs similar tests to those that were demonstrated this morning and would like to add that even though those generally result in our ability to gain root access or other access to systems, we sometimes are just as successful in guessing passwords and using social engineering to gain access to those systems.

Even if agencies do implement the corrective actions that have been identified, all too often subsequent reviews have uncovered the same types of vulnerabilities. As we've reported in the past, these weaknesses continue to exist principally because agencies have not established effective computer security management programs. Effective programs would allow for processes and procedures to assess risks, to ensure that controls are adequately put in place to address those risks, to have a regular process of raising

awareness by the employees, and last, to have a process to monitor the effectiveness of security on an ongoing basis.

While we have seen that some agencies have implemented policies and procedures and have established risk awareness programs, little has been done by most agencies to actively monitor the effectiveness of the controls, unlike what was demonstrated today by the Department of Energy.

The Congress has expressed concern about the serious and pervasive nature of computer security and recently passed legislation that would require some additional reporting and work to be done. Specifically, the legislation requires that agencies establish computer security management programs over all operations and assets of the agency.

Second, the legislation requires both agency and Inspector General annual reviews to be performed, and the information from those reviews could be very helpful in oversight and monitoring of agencies' progress.

Other actions have been initiated across government, including several agencies that have taken important steps to improve computer security. The Federal Chief Information Officers Council has issued a guide for measuring agency progress, which we assisted in developing; and the prior administration has issued a national plan for information systems protection as well as the current administration issuing the first annual update on the status of critical infrastructure.

It is important to maintain the momentum of these efforts and ensure that the activities currently underway are coordinated under a comprehensive strategy and that the roles and responsibilities of the numerous organizations with central responsibilities for computer security are clearly defined.

Mr. Chairman, that concludes our statement. I would be pleased to answer any questions that you or the members of the subcommittee may have.

[The prepared statement of Robert F. Dacey follows:]

PREPARED STATEMENT OF ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, GENERAL ACCOUNTING OFFICE

Mr. Chairman and Members of the Subcommittee: I am pleased to be here today to discuss our analysis of information security audits 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, data tampering, fraud, and inappropriate disclosure of sensitive information.

Today, I will summarize the results of our analysis of information security audits performed by us and by agency inspectors general since July 1999 at 24 major federal departments and agencies. In summarizing these results, I will discuss the types of pervasive weaknesses that we and agency inspectors general have identified. I will then describe the serious risks that these weaknesses pose at selected individual agencies of particular interest to this subcommittee, and the major common weaknesses that agencies need to address. Finally, I will describe the management improvements that are needed to resolve these weaknesses and the significant challenges that remain.

BACKGROUND

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing 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 on a 24-hour-a-day basis; 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 our 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.

Reports of attacks and disruptions abound. The March 2001 report of the "Computer Crime and Security Survey," conducted by the Computer Security Institute and the Federal Bureau of Investigation's San Francisco Computer Intrusion Squad, showed that 85 percent of respondents (primarily large corporations and government agencies) had detected computer security breaches within the last 12 months. Disruptions caused by virus attacks, such as the ILOVEYOU virus in May 2000 and 1999's Melissa virus, have illustrated the potential for damage that such attacks hold.[1] A sampling of reports summarized in Daily Reports by the FBI's National Infrastructure Protection Center[2] during two recent weeks in March illustrates the problem further:

- Hackers suspected of having links to a foreign government successfully broke into the Sandia National Laboratory's computer system and were able to access sensitive classified information. (Source: Washington Times, March 16, 2001.)
- A hacker group by the name of "PoizonB0x" defaced numerous government web sites, including those of the Department of Transportation, the Administrative Office of the U.S. Courts, the National Science Foundation, the National Oceanic and Atmospheric Administration, the Princeton Plasma Physics Laboratory, the General Services Administration, the U.S. Geological Survey, the Bureau of Land Management, and the Office of Science & Technology Policy. (Source: Attrition.org., March 19, 2001.)
- The "Russian Hacker Association" is offering over the Internet an e-mail bombing system that will destroy a persons "web enemy" for a fee. (Source: UK Ministry of Defense Joint Security Coordination Center)
- Two San Diego men allegedly crashed a company's computer system by rerouting tens of thousands of unsolicited e-mails through its servers. (Source: ZDNet News, March 18, 2001.)

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 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, or degrade the integrity of and deny access to data. 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 that information attacks will threaten vital national interests increases. 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 a great deal of knowledge about computer intrusions.

Since 1996, our analyses of information security at major federal agencies have shown that federal systems were not being adequately protected from these threats, even though these systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. In September

---

[1] *Critical Infrastructure Protection: "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities* (GAO/T-AIMD-00-181, May 18, 2000); *Information Security: "ILOVEYOU" Computer Virus Emphasizes Critical Need for Agency and Governmentwide Improvements* (GAO/T-AIMD-00-171, May 10, 2000); *Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection Over Systems and Sensitive Data* (GAO/T-AIMD-99-146, April 15, 1999).

[2] In its Daily Reports, the National Infrastructure Protection Center states that these summaries are for information purposes only and do not constitute any verification of the information contained in the reports or endorsement by the FBI.

1996, we reported that serious weaknesses had been found at 10 of the 15 largest federal agencies, and we concluded that poor information security was a widespread federal problem with potentially devastating consequences.[3] In 1998 and in 2000, we analyzed audit results for 24 of the largest federal agencies: both analyses found that all 24 agencies had significant information security weaknesses.[4] As a result of these analyses, we have identified information security as a high-risk issue in reports to the Congress since 1997-most recently in January 2001.[5]

WEAKNESSES REMAIN PERVASIVE

Evaluations published since July 1999 show that federal computer systems are riddled with weaknesses that continue to put critical operations and assets at risk. Significant weaknesses have been identified in each of the 24 agencies covered by our review. These weaknesses 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 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 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.

Weaknesses in these areas placed a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they placed an enormous amount of highly sensitive data—much of it pertaining to individual taxpayers and beneficiaries—at risk of inappropriate disclosure.

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. While these increases in reported weaknesses are disturbing, they 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, our analysis leaves 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 covered in our analysis 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 the Departments of Defense and 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 systems supporting nonfinancial operations.

In response to congressional interest, during fiscal years 1999 and 2000, we expanded our audit focus to cover a wider range of nonfinancial operations. We expect this trend to continue.

RISKS TO FEDERAL OPERATIONS, ASSETS, AND CONFIDENTIALITY ARE SUBSTANTIAL

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.

---

[3] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996).

[4] *Information Security: Serious Weaknesses Place Critical Fedearl Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998); Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies (GAO/AIMD-00-295, September 6, 2000).

[5] *High-Risk Series: Information Management and Technology* (GAO/HR-97-9, February 1, 1997); *High-Risk Series: An Update* (GAO/HR-99-1, January 1999); *High Risk Series: An Update* (GAO-01-263, January 2001).

The weaknesses identified place a broad array of federal operations and assets at risk of fraud, misuse, and disruption. For example, weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections, and weaknesses at the Department of Defense increase the vulnerability of various military operations. Further, information security weaknesses place enormous amounts of confidential data, ranging from personal and tax data to proprietary business information, at risk of inappropriate disclosure. For example, in 1999, a Social Security Administration employee pled guilty to unauthorized access to the administration's systems. The related investigation determined that the employee had made many unauthorized queries, including obtaining earnings information for members of the local business community.

Such risks, if inadequately addressed, may limit government's ability to take advantage of new technology and improve federal services through electronic means. For example, this past February, we reported on serious control weaknesses in the Internal Revenue Service's (IRS) electronic filing system, noting that failure to maintain adequate security could erode public confidence in electronic filing, jeopardize the Service's ability to meet its goal of 80 percent of returns being filed electronically by 2007, and deprive it of financial and other anticipated benefits. Specifically, we found that, during the 2000 tax filing season, IRS did not adequately secure access to its electronic filing systems or to the electronically transmitted tax return data those systems contained. We demonstrated that unauthorized individuals, both internal and external to IRS, could have gained access to these systems and viewed, copied, modified, or deleted taxpayer data. In addition, the weaknesses we identified jeopardized the security of the sensitive business, financial, and taxpayer data on other critical IRS systems that were connected to the electonic filing systems. The IRS Commissioner has stated that, in response to recommendations we made, IRS has completed corrective action for all of the critical access control vulnerabilities we identified and that, as a result, the electronic filing systems now satisfactorily meet critical federal security requirements to protect the taxpayer.[6] As part of our audit follow up activities, we plan to evaluate the effectiveness of IRS's corrective actions.

I would now like to describe the risks associated with specific recent audit findings at agencies of particular interest to this subcommittee.

• Information technology is essential to the Department of Energy's (DOE) scientific research mission, which is supported by a large and diverse set of computing systems, including very powerful supercomputers located at DOE laboratories across the nation. In June 2000, we reported that computer systems at DOE laboratories supporting civilian research had become a popular target of the hacker community, with the result that the threat of attacks had grown dramatically in recent years.[7] Further, because of security breaches, several laboratories had been forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions. In February 2001, the DOE's Inspector General reported network vulnerabilities and access control weaknesses in unclassified systems that increased the risk that malicious destruction or alteration of data or the processing of unauthorized operations could occur.[8]

• In February, the Department of Health and Human Services' Inspector General again reported serious control weaknesses affecting the integrity, confidentiality, and availability of data maintained by the department.[9] Most significant were weaknesses associated with the department's Health Care Financing Administration, which was responsible, during fiscal year 2000, for processing more than $200 billion in medicare expenditures. HCFA relies on extensive data processing operations at its central office to maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and to process all payments for managed care. HCFA also relies on Medicare contractors, who use multiple shared systems to collect and process personal health, financial, and medical data associated with Medicare claims. Significant weaknesses were also reported for the Food and Drug Administration and the department's Division of Financial Operations.

• The Environmental Protection Agency (EPA) relies on its computer systems to collect and maintain a wealth of environmental data under various statutory and

---

[6] *Information Security: IRS Electronic Filing Systems* (GAO-01-306, February 16, 2001).

[7] *Information Security: Vulnerabilities in DOE's Systems for Unclassified Civilian Research* (GAO/AIMD-00-140, June 9, 2000).

[8] *Report on the Department of Energy's Consolidated Financial Statements*, DOE/IG-FS-01-01, February 16, 2001.

[9] *Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 2000,* A-17-00-00014, February 26, 2001.

regulatory requirements. EPA makes much of its information available to the public through Internet access in order to encourage public awareness of and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality. In July 2000, we reported serious and pervasive problems that essentially rendered EPA's agencywide information security program ineffective.[10] Our tests of computer-based controls concluded that the computer operating systems and agencywide computer network that support most of EPA's mission-related and financial operations were riddled with security weaknesses.

In addition, EPA's records showed that its vulnerabilities had been exploited by both external and internal sources, as illustrated by the following examples.

—In June 1998, EPA was notified that one of its computers was used by a remote intruder as a means of gaining unauthorized access to a state university's computers. The problem report stated that vendor-supplied software updates were available to correct the vulnerability, but EPA had not installed them.

—In July 1999, a chat room was set up on a network server at one of EPA's regional financial management centers for hackers to post notes and, in effect, conduct on-line electronic conversations.

—In February 1999, a sophisticated penetration affected three of EPA's computers. EPA was unaware of this penetration until notified by the FBI.

—In June 1999, an intruder penetrated an Internet web server at EPA's National Computer Center by exploiting a control weakness specifically identified by EPA about 3 years earlier during a previous penetration of a different system. The vulnerability continued to exist because EPA had not implemented vendor software updates (patches), some of which had been available since 1996.

—On two occasions during 1998, extraordinarily large volumes of network traffic—synonymous with a commonly used denial-of-service hacker technique—affected computers at one of EPA's field offices. In one case, an Internet user significantly slowed EPA's network activity and interrupted network service for over 450 EPA computer users. In a second case, an intruder used EPA computers to successfully launch a denial-of-service attack against an Internet service provider.

—In September 1999, an individual gained access to an EPA computer and altered the computer's access controls, thereby blocking authorized EPA employees from accessing files. This individual was no longer officially affiliated with EPA at the time of the intrusion, indicating a serious weakness in EPA's process for applying changes in personnel status to computer accounts.

Of particular concern was that many of the most serious weaknesses we identified-those related to inadequate protection from intrusions through the Internet and poor security planning-had been previously reported to EPA management in 1997 by EPA's inspector general.[11] The negative effects of such weaknesses are illustrated by EPA's own records, which show several serious computer security incidents since early 1998 that have resulted in damage and disruption to agency operations. As a result of these weaknesses, EPA's computer systems and the operations that rely on them were highly vulnerable to tampering, disruption, and misuse from both internal and external sources.

EPA management has developed and begun to implement a detailed action plan to address reported weaknesses. However, the agency does not expect to complete these corrective actions until 2002 and continued to report a material weakness in this area in its fiscal year 2000 report on internal controls under the Federal Managers' Financial Integrity Act of 1982.[12]

• The Department of Commerce is responsible for systems that the department has designated as critical for national security, national economic security, and public health and safety. Its member bureaus include the National Oceanic and Atmospheric Administration, the Patent and Trademark Office, the Bureau of the Census, and the International Trade Administration. During December 2000 and January

---

[10] *Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk* (GAO/AIMD-00-215 July 6, 2000).

[11] *EPA's Internet Connectivity Controls*, Office of Inspector General Report Audit (Redacted Version), September 5, 1997.

[12] *Audit Rewport on EPA's Fiscal 2000 Financial Statements,* Office of the Inspector General Audit Report 2001-1-00107, February 28, 2001.

2001, Commerce 's inspector general reported significant computer security weaknesses in several of the department's bureaus and, last month, reported multiple material information security weaknesses affecting the department's ability to produce accurate data for financial statements. These included a lack of formal, current security plans and weaknesses in controls over access to systems and over software development and changes.[13] At the request of the full committee, we are currently evaluating information security controls at selected other Commerce bureaus.

WHILE NATURE OF RISK VARIES, CONTROL WEAKNESSES ACROSS AGENCIES ARE STRIKINGLY SIMILAR

The nature of agency operations and their related risks vary. However, striking similarities remain in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations—and therefore on what corrective actions they must take. The sections that follow describe the six areas of general controls and the specific weaknesses that were most widespread at the agencies covered by our analysis.

Security Program Management

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 cost effectively, rather than react to individual problems in an ad-hoc manner only after a violation 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 problem. Virtually all of the agencies for which this aspect of security was reviewed had deficiencies. Specifically, many had not developed security plans for major systems based on risk, had not documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. As a result, 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 controls that were not effective, and
- could not make informed judgments as to whether they were spending too little or too much of their resources on security.

With the October 2000 enactment of the government information security reform provisions of the fiscal year 2001 National Defense Authorization Act, agencies are now required by law to adopt the practices described above, including annual management evaluations of agency security.

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 an authenticated user can access and the actions that he or she can execute. Without adequate access controls, unauthorized individuals, including outside intruders and terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. Even authorized users can 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 to keep records of individual users' actions on the com-

[13] *Department of Commerce's Fiscal year 2000 Consolidated Financial Statements, Inspector General Audit Report No. FSD-12849-1-0001.*

puter. Finally, access authorizations and related controls must be maintained and adjusted on an ongoing basis to accommodate new and terminated employees, and changes in users' responsibilities and related access needs.

Significant access control weaknesses were reported for all of the agencies covered by our analysis, as evidenced by the following examples:

- Accounts and passwords for individuals no longer associated with the agency were not deleted or disabled; neither were they adjusted for those whose responsibilities, and thus need to access certain files, changed. At one agency, as a result, former employees and contractors could and in many cases did still read, modify, copy, or delete data. At this same agency, even after 160 days of inactivity, 7,500 out of 30,000 users' accounts had not been deactivated.
- Users were not required to periodically change their passwords.
- Managers did not precisely identify and document access needs for individual users or groups of users. Instead, they provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, all 1,100 users were granted access to sensitive system directories and settings. At another agency, 20,000 users had been provided access to one system without written authorization.
- Use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access. During testing at one agency, we were able to guess many passwords based on our knowledge of commonly used passwords and were able to observe computer users' keying in passwords and then use those passwords to obtain "high level" system administration privileges.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access-control coverage. At one agency data center, all users, including programmers and computer operators, had the capability to read sensitive production data, increasing the risk that such sensitive information could be disclosed to unauthorized individuals. Also at this agency, certain users had the unrestricted ability to transfer system files across the network, increasing the risk that unauthorized individuals could gain access to the sensitive data or programs.

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. Our auditors have been successful, in almost every test, in readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind. Further, user activity was inadequately monitored. At one agency, much of the activity associated with our intrusion testing was not 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.

Application Software Development and Change Controls

Application software development and change controls 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 prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and to ensure that different versions are not misidentified.

Such controls can prevent both 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.

Weaknesses in software program change controls were identified for almost all of the agencies where such controls were evaluated. Examples of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. At another, documentation was not retained to demonstrate user testing and acceptance.

- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally developed" (unauthorized) software programs was prevented or detected.
- Agencies' policies and procedures frequently did not address the maintenance and protection of program libraries.

Segregation of Duties

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, one 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. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

Segregation of duties weaknesses were identified at most of the agencies covered by our analysis. Common problems involved computer programmers and operators who were authorized to perform a variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation.

Segregation of duties problems were also identified related to transaction processing. For example, at one agency, 11 staff members involved with procurement had system access privileges that allowed them to individually request, approve, and record the receipt of purchased items. In addition, 9 of the 11 had system access privileges that allowed them to edit the vendor file, which could result in fictitious vendors being added to the file for fraudulent purposes. For fiscal year 1999, we identified 60 purchases, totaling about $300,000, that were requested, approved, and receipt-recorded by the same individual.

Operating System 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 of the 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 operating system-based security controls 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 of the 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 proc-

essing 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 discussed earlier. 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.

Weaknesses were identified at each of the agencies for which operating system controls were reviewed. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a variety of ways. For example, at one agency, system support personnel had the ability to change data in the system audit log. As a result, they could have engaged in a wide array of inappropriate and unauthorized activity and could have subsequently deleted related segments of the audit log, thus diminishing the likelihood that their actions would be detected.

Further, pervasive vulnerabilities in network configuration exposed agency systems to attack. These vulnerabilities stemmed 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

Finally, service continuity controls ensure that when unexpected events occur, critical operations will continue without undue interruption and that crucial, sensitive data are protected. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations, should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers, as well as the activities performed by users of specific applications. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If 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 financial or management information. Controls to ensure service continuity should address the entire range of potential disruptions. These may include 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.

Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity control weaknesses were reported for most of the agencies covered by our analysis. Examples of weaknesses included 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. At one agency, periodic walkthroughs or unannounced tests of the disaster recovery plan had not been performed. Conducting these types of tests provides a scenario more likely to be encountered in the event of an actual disaster.

IMPROVED SECURITY PROGRAM MANAGEMENT IS ESSENTIAL

The audit reports cited in this statement and in our prior information security reports include many recommendations to individual agencies that address specific weaknesses in the areas I have just described. It is each individual agency's responsibility to ensure that these recommendations are implemented. Agencies have taken steps to address problems and many have good remedial efforts underway. However, these efforts will not be fully effective and lasting unless they are supported by a strong agencywide security management framework.

Establishing such a management framework 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. This cycle of risk management activities is depicted below.

This cycle of activity, as described in our May 1998 executive guide, is consistent with guidance on information security program management provided to agencies by the Office of Management and Budget (OMB) and by NIST. In addition, the guide has been endorsed by the federal Chief Information Officers (CIO) Council as a useful resource for agency managers. We believe that implementing such a cycle of activity is the key to ensuring that information security risks are adequately considered and addressed on an ongoing basis.

While instituting this framework is essential, there are several steps that agencies can take immediately. Specifically, they 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. None of these actions alone will ensure good security. However, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay.

NEW LEGAL REQUIREMENTS PROVIDE BASIS FOR IMPROVED MANAGEMENT AND OVERSIGHT

Due to concerns about the repeated reports of computer security weaknesses at federal agencies, in 2000, the Congress passed government information security reform provisions require agencies to implement the activities I have just described. These provisions were enacted in late 2000 as part of the fiscal year 2001 NationalDefense Authorization Act. In addition to requiring these management improvements, the new provisions require annual evaluations of agency information security programs by both management and agency inspectors general. The results of these reviews, which are initially scheduled to become available in late 2001, will provide a more complete picture of the status of federal information security than currently exists, thereby providing the Congress and OMB an improved means of overseeing agency progress and identifying areas needing improvement.

IMPROVEMENT EFFORTS ARE UNDERWAY, BUT MANY CHALLENGES REMAIN

During the last two years, a number of improvement efforts have been initiated. Several agencies have taken significant steps to redesign and strengthen their information security programs; the Federal Chief Information Officers Council has issued a guide for measuring agency progress, which we assisted in developing; and the President issued a National Plan for Information Systems Protection and designated the related goals of computer security and critical infrastructure protection as a priority management objective in his fiscal year 2001 budget. These actions are laudable. However, recent reports and events indicate that they are not keeping pace with the growing threats and that critical operations and assets continue to be highly vulnerable to computer-based attacks.

While OMB, the Chief Information Officers Council, and the various federal entities involved in critical infrastructure protection have expanded their efforts, it will be important to maintain the momentum. As we have noted in previous reports and testimonies, there are actions that can be taken on a governmentwide basis to enhance agencies' abilities to implement effective information security.

First, it is important that the federal strategy delineate the roles and responsibilities of the numerous entities involved in federal information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible

for overseeing and coordinating federal agency security; and NIST, with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies, such as the CIO Council and the entities created under Presidential Decision Directive 63 on critical infrastructure protection are attempting to coordinate agency initiatives. While these organizations have developed fundamentally sound policies and guidance and have undertaken potentially useful initiatives, effective improvements are not taking place, and it is unclear 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 they enforce these controls. In theory, this 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.

However, our studies of best practices at leading organizations have shown that more specific guidance is important. 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; and help ensure that shared data are appropriately protected. 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.

Third, routine periodic audits, such as those required in the government information security reforms recently enacted, would allow for more meaningful performance measurement. Ensuring effective implementation of agency information security and critical infrastructure protection plans will require monitoring to determine if milestones are being met and testing to determine if policies and controls are operating as intended.

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

Fifth, it is important for agencies to have the technical expertise they need to select, implement, and maintain controls that protect their computer systems. Similarly, the federal government must maximize the value of its technical staff by sharing expertise and information. As the year 2000 challenge showed, the availability of adequate technical expertise has been a continuing concern to agencies.

Sixth, agencies can allocate resources sufficient to support their computer security and infrastructure protection activities. 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, some additional amounts are likely to be needed to address specific weaknesses and new tasks. OMB and congressional oversight of future spending on computer security will be important to ensuring that agencies are not using the funds they receive to continue ad hoc, piecemeal security fixes not supported by a strong agency risk management framework.

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

Mr. GREENWOOD. Thank you, Mr. Dacey.

Mr. Tritak.

TESTIMONY OF JOHN S. TRITAK

Mr. TRITAK. Thank you, Mr. Chairman. I welcome the opportunity to appear before this subcommittee to discuss internal Federal Government efforts in securing its critical infrastructures. I ask that my written statement be introduced into the record at this time.

Mr. GREENWOOD. It will be.

Mr. TRITAK. My opening remarks will focus primarily on those efforts through the end of the Clinton administration. A detailed discussion of those efforts are provided in the President's report to the Congress which was published in January and was prepared both by the National Security Council and my office, the Critical Infrastructure Assurance Office, in coordination with Federal Governments and agencies that actually reported on their activities.

Mr. Chairman, as you know, the administration is currently conducting a thorough review of its critical infrastructure protection policy. While the results of that review are still several weeks away, several things we already know, which I think should be discussed here.

First, President Bush himself has indicated that critical infrastructure protection is important to U.S. Economic and national security and will be a priority of his administration.

Second, and the point goes to remarks made by Congressman Tauzin, National Security Adviser Rice has recently stated with regard to government agency organizations that on the one hand no single government agency can handle all of the critical infrastructure assurance problems for the Federal Government. All agencies are stakeholders and have a role in the solution. That said, however, coordination among governments naturally occurring stovepipes must take place and must take place better than it has in the past. Moreover there must be a common point of contact that is accessible both to private industry and the government, Federal Government, the Congress, and the American people in addressing this issue.

A third point was also made by Dr. Rice. She stated that the Federal Government bears a direct responsibility to ensure that it can deliver essential services and perform critical functions necessary for the Nation's defense, the health and welfare and safety of its citizens. I think this statement deserves a little explanation because it makes a very important point about critical infrastructure policy.

In the first instance, critical infrastructure protection is about assured delivery of vital services that are provided by key sectors of government and the economy, including electric power, oil and gas, telecommunications, banking and finance, transportation, water, health and emergency services. To the extent these infrastructures depend on computer systems and networks to deliver those vital services, and increasingly they do, to that extent critical infrastructure policy must be concerned with computer security and information assurance.

Now, under Presidential directive 63 the previous administration established as one of its goals the achievement of the ability to protect the Nation's critical infrastructures from deliberate attacks. That could significantly diminish the government's ability to perform national security missions and ensure the public health and safety of the American people.

When I first took office, this office, I often asked how are we going to know when we've achieved this goal and what does it take to achieve it. I had more than a passing interest in the question because one of the mandates under PDD-63 for my office is to as-

sist Federal agencies in assessing their dependence on critical infrastructures.

Ultimately, our response was to develop what we call "project matrix." That decision came out of a sense of frustration both within our own office as well as some government agencies asking the question how do we go about doing this, managing this very large problem.

Now project matrix basically takes a systems-analysis approach to the critical infrastructure problem. It starts by asking each participating department and agency what services do you provide that are necessary to the Nation's defense, the orderly functioning of the economy, or the health, welfare and safety of Americans. More importantly, of those services, which if disrupted even for short periods of time could have a significant and immediate impact on the public.

You will note, Mr. Chairman, that there's a time-sensitivity element that is important to our analysis. I have to explain why. We believe that those types of services, those types of critical and time-sensitive services, and the systems that are necessary for their delivery, are at the greatest risk if attacked and therefore deserve priority attention in terms of security. Let me give you an example.

Timely hurricane warnings would be deemed under our approach as a critical service; and, therefore, NOAA's national hurricane warning center would be deemed a critical asset. This is because disruption of timely warnings of hurricanes during a hurricane season could have absolutely catastrophic effects on the public.

The matrix approach requires agencies also to think functionally rather than bureaucratically. It is not enough in the case of the national hurricane warning center to determine whether it alone is secure. So, too, must all the other government and private sector entities necessary to the performance of the center's warning operations be secure as well. In many instances, vital functions performed by one agency depend on services provided by another. Assured delivery of critical services are only as good as the weakest link in the delivery chain.

Having essentially mapped a critical government service across government agencies and between government and the private sector, we are now—agencies are better able then to direct their efforts toward determining whether or not that service is vulnerable to disruption and immediate disruption. Among other things, this sort of approach also helps rationalize the budgetary process and prioritizing your security activities within an agency.

Let me say in conclusion, Mr. Chairman, a number of things. First, critical infrastructure policy is inherently a risk-management problem. A number of people here today have all indicated there's no such thing as perfect security. We need to know what is at risk however; and we need to decide how to manage those risks, balancing costs and consequences.

Also, critical infrastructure protection is concerned with computer security, but it is not synonymous with it. There are very good reasons for having good computer security besides those in support of critical infrastructure policy. We've heard about many. Privacy of data bases that have information about citizens is critical, whether or not it would meet the standard of creating an im-

mediate impact and harm on the public in some broader sense. Protecting classified systems is important regardless of what is contained in them.

Now, how we decide to allocate resources for all computer security demands within the Federal Government is essentially a public-policy choice, a choice the administration is currently weighing in its review. That said, if securing critical government services are to be a priority, particularly time-sensitive ones, then going through a process along the lines I've just described is required. In addition, having identified government—critical government assets essential to delivery of critical services, priority must also be given to assessing their vulnerabilities and developing and implementing remediation plans in those instances where vulnerabilities exist. And I can't overemphasize that last point. Just because a government asset is critical doesn't necessarily mean it's vulnerable to cyberattacks. If it is not connected to the Internet, if it is not connected to any part of the world, it by definition would not be vulnerable to outside attack, putting aside the internal problems you may have with disgruntled employees, which we all acknowledge is a problem.

For example, I use the hurricane warning center as an example of how we go through the analytic process. I didn't by any means want to imply it is necessarily vulnerable to attack. In fact, from what I know, it's quite secure. What is the point, however, and what I wish to leave you with is that unless you know how the government's crown jewels function and how having identified those elements all other relevant government assets and private assets that are essential to the functioning of those crown jewels you don't know whether you're vulnerable or not; and, therefore, you don't know whether you're secure or not against cyber-based attacks.

That concludes my remarks, Mr. Chairman; and I welcome any questions you may have.

[The prepared statement of John S. Tritak follows:]

PREPARED STATEMENT OF JOHN S. TRITAK, DIRECTOR, CRITICAL INFRASTRUCTURE ASSURANCE OFFICE

Mr. Chairman, members of the Subcommittee, it is an honor to appear before you today to discuss the status, as of the time that the Bush Administration took office, of Federal government efforts to secure internal critical systems and infrastructure within Departments and Agencies. These efforts are described in some detail in the *Report of the President of the United States on the Status of Federal Critical Infrastructure Protection Activities, January 2001.*

This Subcommittee has shown exceptional leadership on a broad range of national and economic security issues and I am grateful for the opportunity to work closely with you and the Congress to find ways to advance infrastructure assurance for all Americans. As you know, the Bush Administration currently is conducting a thorough review of our critical infrastructure protection policy. We expect the results of that review over the next couple of months. President Bush has indicated already, however, that securing our nation's critical infrastructures will be a priority of his Administration. Your decision to hold this hearing could not be more timely. We all recognize that no viable solutions will be developed or implemented without the executive and legislative branches working together.

I believe the work of your subcommittee, along with that of others, will make an important contribution to establishing a new consensus on safeguarding critical government services against cyber attacks.

BACKGROUND

America has long depended on a complex of systems—or critical infrastructures—to assure the delivery of services vital to its national defense, economic prosperity, and social well-being. These infrastructures include telecommunications, water supplies, electric power, oil and gas delivery and storage, banking and finance, transportation, and vital human and government services.

The Information Age has fundamentally altered the nature and extent of our dependency on these infrastructures. Increasingly, our government, economy, and society are being connected together into an ever expanding and interdependent digital nervous system of computers and information systems. With this interdependence come new vulnerabilities. One person with a computer, a modem, and a telephone line anywhere in the world potentially can break into sensitive government files, shut down an airport's air traffic control system, or cause a power outage in an entire region.

Events such as the 1995 bombing of the Murrah Federal Building in Oklahoma City demonstrated that the Federal government needed to address new types of threats and vulnerabilities, many of which the nation was unprepared to defend against. In response to the Murrah Building tragedy and other events, an interagency working group was formed to examine the nature of the threat, our vulnerabilities, and possible long-term solutions for this aspect of our national security. The National Security Council's Critical Infrastructure Working Group (CIWG) included representatives from the defense, intelligence, law enforcement and national security communities. The working group identified both physical and cyber threats and recommended formation of a Presidential Commission to address more thoroughly many of these growing concerns.

In July 1996 the President's Commission on Critical Infrastructure Protection (PCCIP) was established by Executive Order 13010. The bipartisan PCCIP included senior representatives from private industry, government, and academia; its Advisory Committee consisted of industry leaders who provided counsel to the Commission.

After examining infrastructure issues for over a year, the Commission issued its report, *Critical Foundations: Protecting America's Infrastructures.* The Report reached four significant conclusions:

- First, critical infrastructure protection is central to our national defense, including national security and national economic power;
- Second, growing complexity and interdependence between critical infrastructures may create the increased risk that rather minor and routine disturbances can cascade into national security emergencies;
- Third, vulnerabilities are increasing steadily and the means to exploit weaknesses are readily available; practical measures and mechanisms, the Commission argued, must be urgently undertaken before we are confronted with a national crisis; and
- Fourth, laying a foundation for security will depend on new forms of cooperation with the private sector, which owns and operates a majority of these critical infrastructure facilities.

PDD-63

On May 22, 1998, Presidential Decision Directive 63 (PDD-63) was issued to achieve and maintain the capability to protect our nation's critical infrastructures from acts that would significantly diminish the abilities of:

- The Federal government to perform essential national security missions and to ensure the general public health and safety;
- State and local governments to maintain order and to deliver minimum essential public services; and
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

To achieve these ends, PDD-63 articulates a strategy of:

- Creating a public-private partnership to address the problem of information technology security;
- Raising awareness of the importance of cyber security in the government and in the private sector;
- Stimulating market forces to increase the demand for cyber security and to create standards or best practices;
- funding or facilitating research into new information technology systems with improved security inherent in their design;

- Working with educational facilities to increase the number of students specializing in cyber security; and
- Helping to prevent, mitigate, or respond to major cyber attacks by building an information sharing system among government agencies, among corporations, and between government and industry.

The Federal government's basic approach to critical infrastructure protection, as reflected in PDD-63, has been built around a strong policy preference for consensus-building and voluntary cooperation rather than regulatory actions. In an economy as complex as ours, and with technology changing as quickly as it is, cooperation offers the best and surest way to achieve our shared goals in this emerging area. However, the government's approach also recognizes the need for coordinated actions to improve its internal defenses and the nation's overall posture against these new threats.

PDD-63 called for the Federal government to produce a detailed plan to protect and defend the nation against cyber disruptions. Version 1 of this effort, entitled *The National Plan for Information Systems Protection,* was released in January 2000, and represents the first attempt by a national government to design a comprehensive approach to protect its critical infrastructures. This initial version of the plan focused mainly on domestic efforts being undertaken by the Federal government to protect the nation's critical cyber-based infrastructures. The next version of the plan, due out this summer, will focus on the efforts of the infrastructure owners and operators, as well as the risk management and broader business community.

Under PDD-63, Federal Agencies have a number of distinct responsibilities:

- All agencies are required to protect their own internal critical infrastructures, especially their cyber systems.
- Some agencies with special expertise or functional responsibilities are tasked with providing services to the government as a whole.
- A number of agencies also are charged with developing partnerships with private industry in their sectors of the economy.

I will focus the remainder of my remarks on the first responsibility—securing internal critical systems. Specifically, I will discuss the work of my office, the Critical Infrastructure Assurance Office, in assisting agencies to identify and prioritize these systems. I also will discuss briefly Federal Government efforts to formulate security and best practices standards that apply to information, security, and critical infrastructure assets.

Time constraints prevent me from fully describing the internal efforts of each federal agency to secure their critical systems. I urge the subcommittee to review the status reports of each Department and Agency provided in Section III of the President's *January* Report. Likewise, I strongly recommend that the subcommittee study the agencies' sector partnership efforts described in Section II of the *Report.* These efforts are as important to overall national critical infrastructure assurance as the internal activities that have been undertaken within the Federal government. I would welcome the opportunity to brief the sub-committee on another occasion on the work of the CIAO and the federal lead agencies (Commerce, Energy, Treasury, Transportation, Justice, Health and Human Services, EPA and Defense) in promoting meaningful public-private partnerships.

IDENTIFYING CRITICAL FEDERAL INFRASTRUCTURES AND SYSTEMS: PROJECT MATRIX

In response to PDD 63, my office established Project Matrix last year to "coordinate analyses of the U.S. Government's own dependencies on critical infrastructures."

This is a government-wide issue. Federal Departments and Agencies do not operate independently of one another. Due to significant advances in information technology, the public and private sectors have become inextricably intertwined. As a result, there is limited utility in each Federal Department and Agency viewing physical and cyber security only in the context of its own organization. Project Matrix provides each Federal Department and Agency an expanded, more comprehensive, realistic, and useful view of the world within which it actually functions. The Administration, Congress, and private sector providers of the nation's critical infrastructures will require such information to implement cost efficient and effective physical and cyber security enhancement measures in the future. Project Matrix provides a common methodology and approach and allows the government to develop a clearer picture of cross-agency interdependencies.

Participating in Project Matrix helps each Federal Department and Agency identify the assets, nodes and networks, and associated infrastructure dependencies and interdependencies that are required for it to fulfill its national security, economic

stability, and critical public health and safety responsibilities to the American people. A number of Departments and Agencies refer to Project Matrix in their reports.

Project Matrix also helps each participating Federal Department and Agency:

- Identify the nodes and networks that should receive robust cyber and physical vulnerability assessments;
- Conduct near-term risk management assessments;
- Justify funding requests for high-priority security enhancement measures in the areas of physical security, information system security, industrial security, emergency preparedness, counter-intelligence, counter-terrorism; and
- Review actual business processes to better understand and improve the efficiencies of its organization's functions and information technology architectures.

Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and prioritizes each Federal Department's and Agency's PDD 63 relevant assets. In Step 2, the team provides a business process topology on, and identifies significant points of failure associated with, each Department's or Agency's most critical assets. In Step 3, the team identifies the infrastructure dependencies associated with select assets identified in Step 1 and analyzed in-depth in Step 2.

In FY 2001, the Project Matrix team will complete the documentation of its entire analytical process for use throughout the public and private sectors, improve its Step One automated data collection tool, and develop compatible automated Step Two and Three tools.

INTEGRATING SECURITY INTO THE CAPITAL PLANNING AND BUDGET PROCESSES

In February 2000, OMB issued important new guidance to the agencies on incorporating and funding security in information technology investments. In brief, this policy states that funding will not be provided for agency requests that fail to demonstrate how security is built into and funded as part of each system.

This policy carries through on the requirements of the Clinger-Cohen Act of 1996 and emphasizes that security must be incorporated in and practiced throughout the life cycle of each agency's system and program. To accomplish this, beginning with the FY 2002 budget, each agency budget request to OMB for information technology funding must, among other things:

- Demonstrate life cycle security costs for each system;
- Include a security plan that complies with applicable policy;
- Show specific methods used to ensure that risks are understood, continually assessed, and effectively controlled; and
- Demonstrate that security is an integral part of the agency's enterprise architecture including interdependencies and interrelationships.

THE GOVERNMENT INFORMATION SECURITY REFORM ACT

On October 30, 2000 the President signed into law the FY 2001 Defense Authorization Act (P.L. 106398) including Title X, subtitle G, "Government Information Security Reform (Security Act)." The security provision amends the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35) and primarily addresses the program management and program evaluation aspects of security.

In concert with OMB policy, the Security Act requires agencies to incorporate and practice risk-based and cost-effective security throughout the life cycle of each agency system and thus firmly ties security to the agencies' capital planning and budget processes.

The Security Act also requires on an annual basis:

- Agency program reviews;
- Inspector General evaluations of agency security programs;
- Agency reports to OMB; and
- An OMB report to Congress.

The annual review and reporting requirements will promote consistent, ongoing assessments of government security performance. Recently a uniform method for agency program reviews has been developed.

THE CIO AND CFO COUNCILS: STANDARDS AND BEST PRACTICES

Standardizing the security controls for government systems has a conceptual appeal because it can reduce the complexity and expense of developing, implementing, and monitoring security on a system-by-system basis. This is increasingly important given the government's shortage of expert information security personnel. Government computer security almost certainly would improve if specific standards were prescribed and implemented for each government information system.

However, specific standards for all systems—a "one-size-fits-all" security approach—may not accommodate the vastly different operational requirements of each information system and could unnecessarily impede business operations. Executive branch agencies operate more than 26,000 major information systems, many of which directly interact with the public, industry, or State and local governments. Just as each system has its own unique operational requirements, so too are its security requirements unique.

The CIO Council and the CFO Council recognize both the benefits and potential problems with standardized security approaches. They have undertaken the following important initiatives:

Securing Electronic Government Transactions to the Public—Resource Guide: The CIO Council, the CFO Council, and the Information Technology Association of America are working together to develop a benchmark for risk-based, cost-effective security for three types of electronic government services:

- Web-based information services;
- Government procurement; and
- Financial transactions with the public.

A resource guide for securing electronic transactions with the public will be released in 2001 to assist agency CIOs in promoting electronic government initiatives within their agencies. Together with the CFO Council initiative for agency financial systems, this effort may prove to be an effective pilot for establishing similar benchmarks for other discrete classes of programs and information systems.

Best Security Practices: The CIO Council, led by the U.S. Agency for International Development and NIST, has developed a web-based repository of sound Federal agency security practices that have worked in the real world. The CIO Council's Best Security Practices initiative collects, documents, and disseminates these practices to help agencies reduce the cost of developing and testing new security controls, improve the speed of implementation, and increase the quality of their security programs.

The goal is to populate the repository with more than 100 practices by mid 2001 and continually expand offerings from then on. In their guidance to the agencies on implementing the Government Information Security Reform Act, OMB has instructed agencies to use the CIO Council's best practices initiative to fulfill the new act's requirement to share best practices.

Measuring Performance—Federal Information Technology Security Assessment Framework: Over the past year, the CIO Council, working with NIST, OMB, and the GAO, developed the Federal Information Technology Security Assessment Framework. The framework, issued in December 2000, provides agencies with a self-assessment methodology to determine the current status of their security programs and, where necessary, establish a target for improvement. In developing the framework, the CIO Council recognizes that the security needs for the tens of thousands of Federal information systems differ and must be addressed in different ways.

The framework comprises five levels to guide agency self assessments and to assist them in prioritizing efforts for improvement:

- Level 1 reflects a documented security policy;
- Level 2 shows documented procedures and controls to implement the policy;
- Level 3 indicates that the procedures and controls have in fact been implemented;
- Level 4 shows that the procedures and controls are continually tested and reviewed; and
- Level 5 demonstrates that procedures and controls are fully integrated into a comprehensive program.

Each level represents a more complete and effective security program. Agencies should bring all systems and programs to level 4 and ultimately level 5. OMB and the CIO Council have alerted agencies that when individual systems do not meet the framework's level 4 requirements, the system may not meet OMB's security funding criteria.

As mentioned earlier, the new Government Information Security Reform Act emphasizes the importance of assessing security effectiveness and requires annual agency reporting to OMB of the results of the agency security reviews. OMB has instructed agencies to use the framework to fulfill their assessment and reporting obligations under the Security Act.

CONCLUSION

While much has been accomplished in recent years, much more needs to be done to ensure our critical government systems are adequately protected from cyber attack. I look forward to working with members of this subcommittee, and the entire Congress, as we address the challenges ahead. I look forward to your questions.

Mr. GREENWOOD. Thank you. Appreciate your testimony.

I will direct some questions to Mr. Dacey, if I may. Overall, if you had to give the Federal agencies the GAO has reviewed a collective grade A through F, i.e., passing or failing, how would you rate them as a group?

Mr. DACEY. I think overall the types of weaknesses we've seen, again, are pervasive. In terms of a grade, I'll leave that to Chairman Horn. He's given grades last year, and I am not sure they've changed a whole lot since then.

Mr. GREENWOOD. Would this grade be different for defense versus military agencies than civilian agencies? How would you compare them?

Mr. DACEY. I just wanted to clarify, the main part of the work that's been done has been on unclassified systems. So with respect to those, we're finding similar types of vulnerabilities in both.

Mr. GREENWOOD. The committee's reviews of computer security at various Federal agencies has largely found that security has been mostly a paperwork exercise up to now. Do you agree with that?

Mr. DACEY. There are certain areas, I guess, in terms of a paperwork exercise, that there are documented policies in many cases that aren't carried through in terms of execution. Also, there are many places where the policies aren't even documented. One of the areas that we look at is, again, whether the agencies have a process such as Energy to really determine what the effectiveness of their controls are. We've many times identified vulnerabilities for the first time to agencies; and although they have been generally very responsive, it's a process that we think ought to take place in the management role, not as an audit function. So that is, I guess, how I'd answer that question.

Mr. GREENWOOD. It's safe to say that every agency ought to be constantly testing its own security systems; isn't that a fair statement?

Mr. DACEY. I think there needs to be a regular process for that type of testing. Part of that is called for in the new legislation. The reports on that new legislation will be due out in the fall to Congress, and those should illustrate some of the issues and also indicate whether, in fact, that testing is being done. I believe in your opening statement you referred to the fact, based on evidence you obtained, that that wasn't being done. That is consistent with our—what we have seen actually. We've seen very little done by most agencies to assess the effectiveness of their security.

Mr. GREENWOOD. You mentioned in your testimony some examples of unauthorized access, security breaches, compromised networks and data from GAO's body of work across Federal agencies. These are not just hypothetical, are they?

Mr. DACEY. No. We have seen incidents where that has actually occurred, which I gave in my oral statement. The question really too is some of these vulnerabilities are, or were, sensitive when we found them, at least could have led to all kinds of other things that weren't detected. I would agree based upon the comments earlier that a large number of incidents that are occurring are probably not detected and reported. That is an area where we really need to get better systems because you can't protect the systems a hun-

dred percent, as was discussed earlier; but you need to do the best you can to really implement known patches and address known vulnerabilities. Many of the tools and Web sites that were referred to earlier that provide evidence of ways in which systems can be hacked can also be used by agencies to identify those same types of weaknesses in their system and fix them. So I think that is an important area that needs to be addressed.

Mr. GREENWOOD. It seems to me, as I think Ms. McDonald said, they encourage the use of patches; but there's no requirement that the patches be used, and perhaps we ought to consider a mechanism to make them mandatory.

Mr. Tritak, could you describe for the committee a worst-case scenario for a cyberattack or information-warfare attack on one of our Nation's critical infrastructures, just to make us all feel good?

Mr. TRITAK. Yeah, make me feel real good. If I may a little bit, sir, sort of qualify my remarks by saying the following: I've heard conversations earlier talk about cyberterrorism, information warfare; and that is a shorthand that we all use in describing certain types of threats. I think I prefer when I address these things is to turn around a little bit and not using cyberadjectives to modify traditional nouns but to say in a sense, for example, instead of cyberterrorism, I refer to it as terrorist activities that attempt to exploit cyberspace to achieve certain terrorist goals and objectives. Okay. And in an information warfare context, I think if we're using the term properly, we're in a state of war in which a country is utilizing or exploiting the cyberspace and vulnerabilities in the cyberspace to achieve certain goals and certain objectives.

Now let me give you an idea of the kinds of things I think would be played out in that context. Let's pretend we go back, and we have to, God forbid, have to deal with Iraq again in a way that we had to deal with Iraq before. I think Iraq and the leadership of Iraq probably would prefer not to have to go toe to toe with the Americans the way it had to go toe to toe the first time around. One of the things it probably would attempt to do if it could—and I'm not saying any of this they can actually achieve, because I think it is very difficult to do this, but let's just suppose the intent would be to disrupt the deployment—mobilization and deployment of U.S. Forces in the United States and project them overseas and then also the logistics efforts going from Europe points of demarcation in Europe finally to the Middle East. To the extent they could achieve something like that, it could have strategic implications. So I think we need to look at it in that sense.

Now if you're talking about in the case of a war where in a sense they would attempt to achieve through cyberattacks what bombers used to achieve, for example, then you would think of things that could cause mass problems, disruptions of 911, introduction of biological chemical weapons at the same time, the possibility of trying to hack into dams and potentially open floodgates, anything that would cause the kind of hysteria and potential loss of life that we tried to do in World War II or whatever.

That is the kind of thing I think we all have to be concerned about because I think that is the sort of thing people would be thinking about if they were going to war with us and they wanted to exploit the cyberspace in order to achieve their military and po-

litical objectives. I want to also emphasize it's not clear that they could achieve that; and in fact, this the beauty of now as well as the curse of today is the fact that we haven't seen the worst because the worst that can be done over cyberspace is a function of interconnectivity and being hooked in. And we're still in the fairly early stages of doing this. Our society, our government, our economy are being transformed by information technologies; and increasingly we're going to be depending on wireless technologies in addition to the online versions.

So I think that over time the potential for serious problems conducted over cyberspace will go up. That is why I applaud the efforts that you're trying to do now. Let's not wait for that eventuality. Let's take aggressive action now and perhaps preempt the problem altogether.

Mr. GREENWOOD. Well, while these worst-case scenarios are theoretical, the fact of the matter is would you agree with us that the only thing that stands between us and the worst-case scenario is the extent to which the Federal agencies involved utilize the billions of dollars that we've appropriated to them and the tools, the technological tools that are available to protect against those scenarios?

Mr. TRITAK. Yes. I think that to the extent that Federal agencies are increasingly relying on information technology to do key services in national defense and to the extent that those services are linked into the ever-expanding digital nervous system that is spanning the country and the globe, you are exposing yourself to a risk that you have never had before; and if you are not safeguarding yourself against that, the potential for the kinds of concerns that you have, I think, can't be ignored.

Mr. GREENWOOD. The means will always be there; the motivation will always be there. The only protection is the security systems, and the only long-range protection against those scenarios is constant vigilance, constant testing of our systems to protect us.

Mr. TRITAK. Yes.

Mr. GREENWOOD. Okay. A recent report by a committee of Inspectors General issued just last week found PDD-63 implementation to be progressing very slowly at most Federal agencies. They surveyed 15 Federal agencies including some key ones for PDD-63 purposes and found that quote "many agency infrastructure plans were incomplete," that quote "most agencies had not identified their critical assets yet and that almost none of the agencies had completed vulnerability assessments of those assets or developed remediation plans." Do you concur, Mr. Tritak, with this assessment, and why are we so far in the hole on this?

Mr. TRITAK. Well, a couple things. I think that there's some truth to what you have said. I can't articulate for you in full to what extent that is the case in each agency situation. What I can tell you is in the case of the work that we're doing with agencies under the project matrix all efforts that have been done so far are in the area of identifying the assets.

I just want to qualify one piece about that because some of these assets may have been assessed for vulnerabilities during Y2K, for example, and for other reasons—and we can't necessarily assume that nothing has been done—but I think one of the points I am try-

ing to get across to this committee is unless you understand the full—the way the systems operate in critical services and you have addressed every single aspect of that service for vulnerabilities, you don't know whether that service is assured or not. I think in that regard we have a long way to go, a real long way to go.

Mr. GREENWOOD. Okay. We thank you both for your testimony. The Chair seeks unanimous consent that documents that have been agreed to by the staff majority and minority be admitted into the record and that the record remain open for 30 days for additional statements and materials. With that, this committee thanks all of its witnesses and adjourns.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

CRYPTEK
SECURE COMMUNICATIONS, LLC
April 5, 2001

The Honorable W.J. "BILLY" TAUZIN
Chairman
House Energy and Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515-6115

DEAR MR. CHAIRMAN, I am submitting the following testimony and presentation for the record at the suggestion of Mr. Gary A. Dionne, a member of your Committee's professional staff. My firm is the developer and manufacturer of a network security product known as Diamond*TEK*.™ Diamond*TEK* is the only network security component to ever successfully complete the National Security Agency's (NSA) B2 level evaluation. What this means is that Diamond*TEK* is approved by the NSA to handle data of multiple levels of classification on a single workstation over a single network connection. This can translate in significant cost savings for government users who must worry about keeping data of various classification levels separate and secure.

This technology is also invaluable to users of sensitive, valuable data in the commercial marketplace. An example that comes immediately to mind is ensuring the confidentiality of patient medical records. Another industry that could benefit from such technology is the financial services industries and any organization involved with funds transfer. One misplaced "byte" could mean the loss of billions of dollars.

Cryptek developed Diamond*TEK* with internal R&D funds to meet stringent NSA requirements. The company has continued to invest in the technology, resulting in the worlds most "trusted" and secure network security product. This leading edge capability is available today for government and commercial users worldwide (Cryptek recently received a blanket export license from the Department of Commerce to export to any commercial or government entity in the world with the exception of the seven terrorist-sponsoring nations).

I wanted to ensure that the Committee was aware that this technology was available as you consider various encryption and privacy issues during this Congress. Cryptek stands prepared to brief you, other Committee Members or staff on our unique products and capabilities and answer questions you may have.

Thank you for your consideration of this information.

Sincerely,

JACKSON KEMPER, III
Vice President, Government Affairs

CRYPTEK

SECURE COMMUNICATIONS, LLC

14130-C Sullyfield Circle
Chantilly, Virginia 20151

(703) 652-0125

Submission for the Record

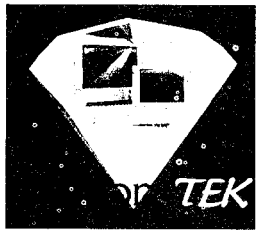
House Committee on Energy and Finance

April 5, 2001

CRYPTEK
SECURE COMMUNICATIONS, LLC

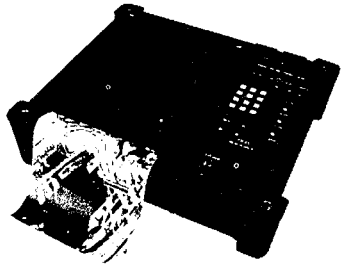
The Company

15 years providing secure products to U.S. & foreign governments. Two major product areas:



NSA-evaluated network security products. LAN product has passed B2 level evaluation by NSA.

WAN product in Common Criteria process.



TS-21 Blackjack Tactical Computer Peripheral

Approximately 6,000 secure FAX products delivered

CRYPTEK
SECURE COMMUNICATIONS, LLC

Cryptek Mission

To provide military grade network security products to commercial markets that are cost effective and easy to install and operate.

CRYPTEK
SECURE COMMUNICATIONS, LLC

Cryptek Mission

To provide military grade network security products to commercial markets that are cost effective and easy to install and operate.

CRYPTEK
SECURE COMMUNICATIONS, LLC

CRYPTEK'S Approach to Network Security: DiamondTEK

- Network Security is rapidly growing market: we are a totally unique approach with no direct competition.

- DiamondTEK is a revolutionary product: developed with and evaluated by the National Security Agency (NSA) to be a "total" network security solution.

- We have taken this product, developed with the NSA, and made it available to government-wide and commercial markets.

- Because of our NSA B2 evaluation, users can be assured that our solution is "hack proof," a claim no competitor can make.

CRYPTEK SECURE COMMUNICATIONS, LLC DiamondTEK ® - A New Class of Product

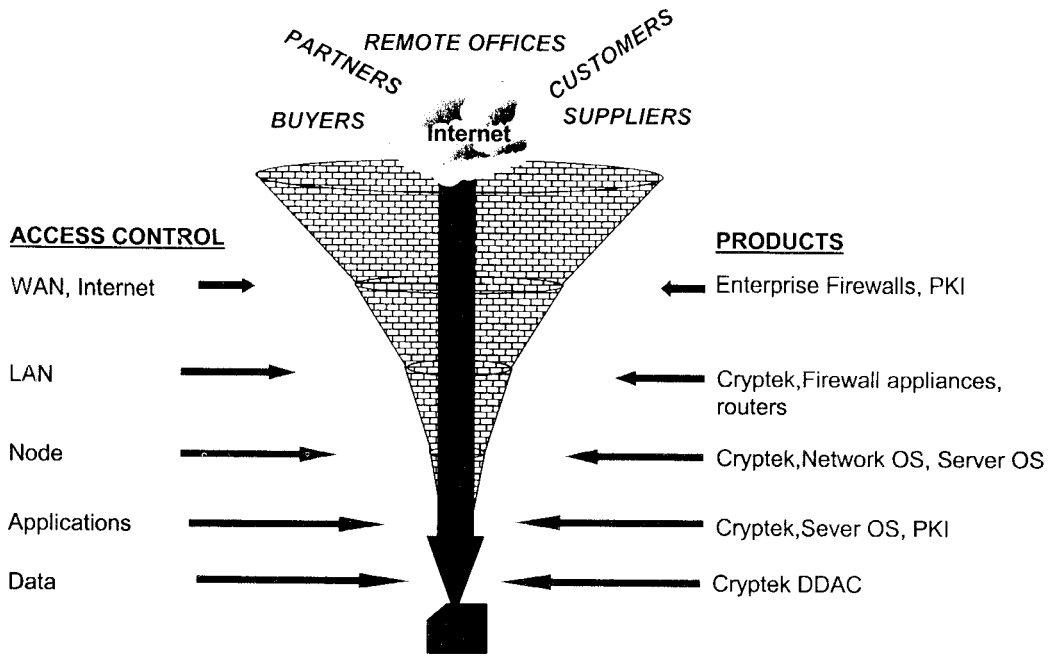
- Combines most important security functions in one appliance
  - Token-based user I&A and full-path IPSec
  - Distributed packet filtering firewall and intrusion detection
  - Centralized audit and role based access control
- Network appliance
  - "Drop in" component transforms network into a security device
  - Dynamic Secure Virtual Networks™
- Self-protecting security processor embedded in a network component
  - High penetration resistance and performance
  - Operating system independence, legacy system compatibility
- New Data Driven Access Control (DDAC)™ technology
  - Network infrastructure and data collaborate to control data transfers
- Evaluated by the National Security Agency for high trust

CRYPTEK
SECURE COMMUNICATIONS, LLC

Unique DiamondTEK® Benefits

- Unique security capabilities
  1. Makes the Internet safe for business
  2. Hardens networks against penetration and disruption
  3. Makes network security applications-aware
  4. Data and the network determine to whom and where data can go
  5. Easy to use and deploy appliance
  6. Secures network close to the data where security works best
  7. Unburdens users from primary responsibility for security
  8. Protects servers from errors in security configuration
  9. Prevents unauthorized access using stolen passwords
  10. Protects all types of networked equipment and applications

CRYPTEK SECURE COMMUNICATIONS, LLC Security Is Access Control

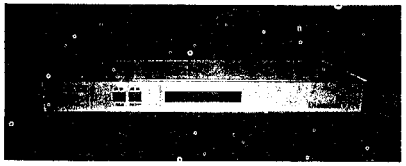


CRYPTEK SECURE COMMUNICATIONS, LLC Competitive Products

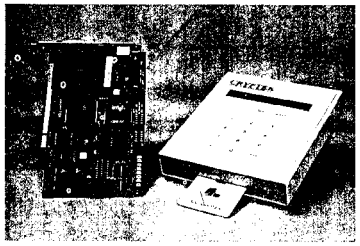
[illegible]	[illegible]	[illegible]
Firewall (FW) and VPNs	Control access to network and protect external communication	NAI, Cisco, Lucent, Axent, SonicWall, Intel
[illegible]	Identify and [illegible] users and their public [illegible] keys. (Requires [illegible] applications)	[illegible] Technologies [illegible]
Intrusion Detection (ID)	Monitors application access to detect intrusion attempts	ISS, Axent, CheckPoint
IP Security [illegible] FW, VPN, [illegible]	Protect network servers and data	[illegible]

CRYPTEK SECURE COMMUNICATIONS, LLC

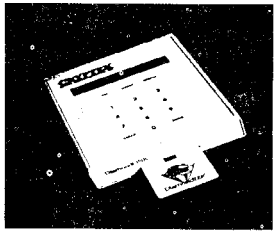
DiamondTEK Family



DiamondVPN protects workgroups or entire networks.



Internal DiamondNIC and attached authentication card readers protect a single computer.



External Diamond*Link*™ is the preferred appliance. Ideal for legacy systems and networked equipment.

CRYPTEK SECURE COMMUNICATIONS, LLC Cryptek Alliance Partners

TELOS e-Solutions for Connected Enterprises

CSI DATA·SYSTEMS

ca Computer Associates

AMSEC

LOCKHEED MARTIN

VERIDIAN

gtsi.com

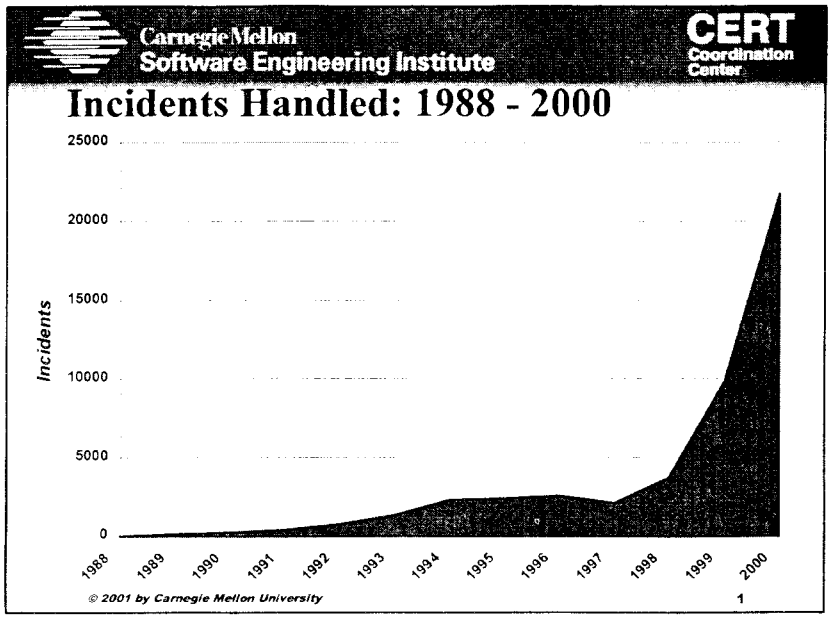
Areall SERVICES

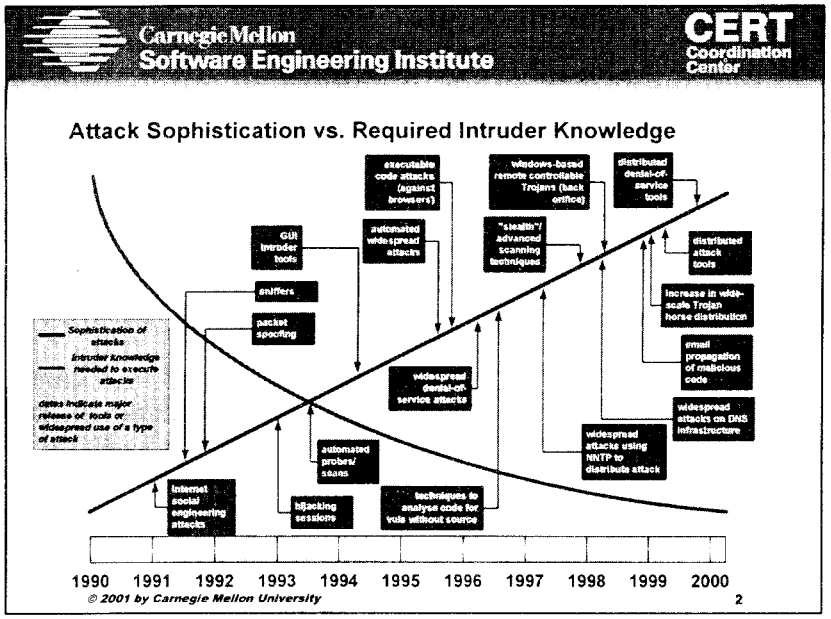
EuroTelecom

Cyber Attack: Rapid Response for Critical Infrastructure Protection

General Services Administration
Federal Technology Service

Carnegie Mellon University
Software Engineering Institute

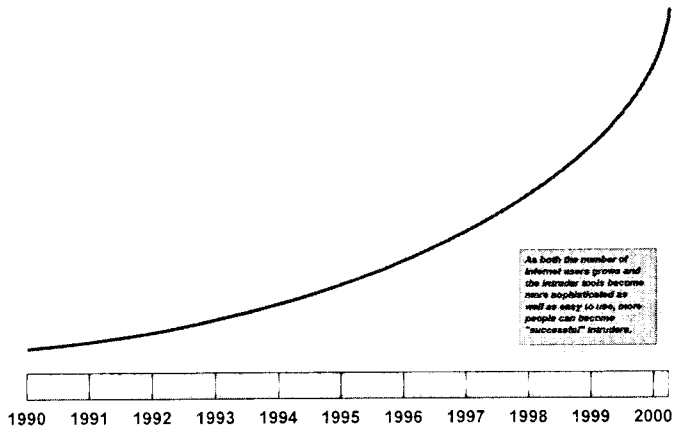

Carnegie Mellon
Software Engineering Institute
CERT
Coordination Center
Incidents Handled: 1988 - 2000
Incidents
25000
20000
15000
10000
5000
0
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
© 2001 by Carnegie Mellon University
1


Carnegie Mellon
Software Engineering Institute
CERT
Coordination Center
Attack Sophistication vs. Required Intruder Knowledge
executable code attacks (against browsers)
windows-based remote controllable Trojans (back orifice)
distributed denial-of-service tools
GUI intruder tools
automated widespread attacks
"stealth"/ advanced scanning techniques
distributed attack tools
sniffers
Increase in wide-scale Trojan horse distribution
packet spoofing
email propagation of malicious code
widespread denial-of-service attacks
widespread attacks on DNS infrastructure
widespread attacks using NNTP to distribute attack
automated probes/ scans
Internet social engineering attacks
hijacking sessions
techniques to analyze code for vuln without source
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
© 2001 by Carnegie Mellon University
2

Carnegie Mellon
Software Engineering Institute

CERT
Coordination Center

Number of Intruders Able to Execute Attacks



© 2001 by Carnegie Mellon University

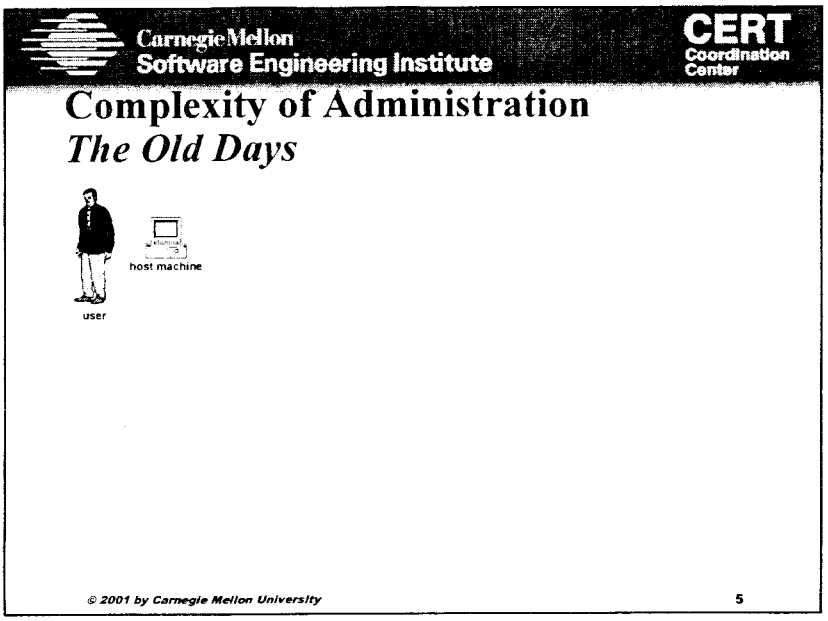
Carnegie Mellon
Software Engineering Institute

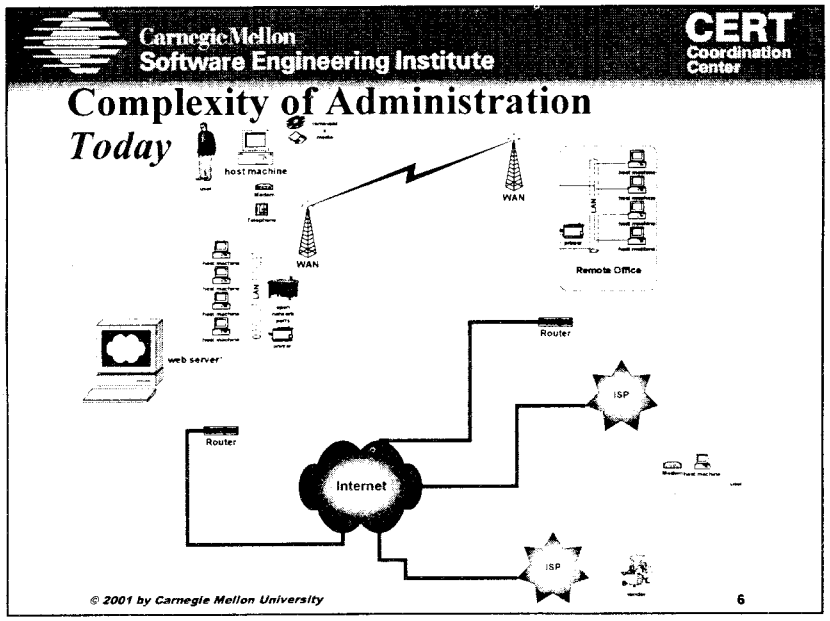
CERT
Coordination Center

Can Many Intrusions be Prevented?

of intrusions result from exploitation of known vulnerabilities or configuration errors where countermeasures were available.

© 2001 by Carnegie Mellon University

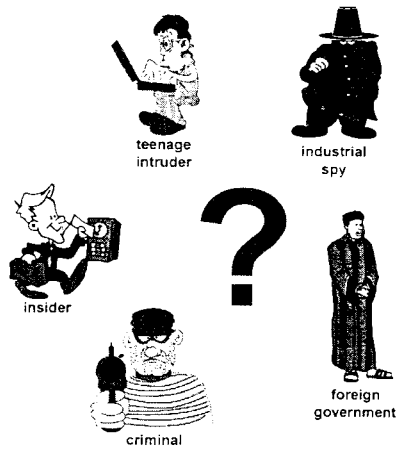

Carnegie Mellon
Software Engineering Institute
CERT
Coordination Center
Complexity of Administration
The Old Days
host machine
user
© 2001 by Carnegie Mellon University
5


Carnegie Mellon
Software Engineering Institute
CERT
Coordination Center
Complexity of Administration
Today
host machine
WAN
WAN
Remote Office
Router
web server
ISP
Router
Internet
ISP
© 2001 by Carnegie Mellon University
6

Carnegie Mellon
Software Engineering Institute

CERT
Coordination Center

Who is Attacking Systems?



© 2001 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

CERT
Coordination Center

Threat Pyramid

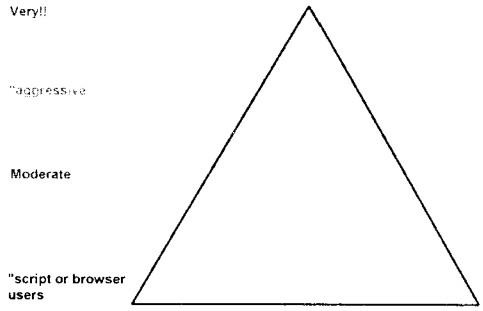


Diagram courtesy Tom Perrine
San Diego Supercomputer Center

© 2001 by Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute
CERT Coordination Center

Direction of Internet Security (1)

What the Internet community is facing in terms of Internet security in the next few years can be summed up in the following statements:

- the expertise of intruders is increasing
- the sophistication of attacks and intruder tools/toolkits is increasing
- the effectiveness of intruders is increasing (*knowledge is being passed to less knowledgeable intruders thus making them effective*)

© 2001 by Carnegie Mellon University 9

Carnegie Mellon
Software Engineering Institute
CERT Coordination Center

Direction of Internet Security (2)

- the number of intrusions is increasing
- the number of companies and users of the Internet is increasing
- the complexity of protocols and applications run on clients and servers attached to the Internet is increasing
- the complexity of the Internet as a network is increasing

© 2001 by Carnegie Mellon University 10

Direction of Internet Security (3)

- the information infrastructure has many fundamental security design problems that cannot be quickly addressed
- the number of people with security knowledge and expertise is increasing, but at a significantly smaller rate than the increase in the number of Internet users
- the number of security tools available is increasing, but not necessarily as fast as the complexity of software, systems and networks

© 2001 by Carnegie Mellon University

Direction of Internet Security (4)

- the number of incident response teams is increasing, but the ratio of incident response personnel to Internet users is decreasing
- the vendor product development and testing cycle is decreasing
- vendors continue to produce software with vulnerabilities, including types of vulnerabilities where prevention is well-understood *(such as buffer overflows)*

© 2001 by Carnegie Mellon University

GSA

FTS

Federal Computer Incident Response Center (FedCIRC)

U. S. General Services Administration
Federal Technology Service

GSA

FedCIRC Mission

FedCIRC is the government's focal point for handling computer security related incidents. It provides incident detection, containment and recovery assistance to civilian agencies and departments of the Federal Government that have experienced a computer security related event and disseminates security relevant information, tools and advice for the protection of information technology resources and information.

U. S. General Services Administration
Federal Technology Service

GSA

FedCIRC Chronology

Feb 1996	• OMB Circular A-130 (Appendix III)
Oct 1997	• NIST develops FedCIRC pilot program under funding from GITS board
Feb 1998	• CIO Council requests GSA assume FedCIRC operational responsibilities
Mar 1998	• CIO Council announces sponsorship for FedCIRC
May 1998	• FedCIRC operational charter published • PDD-63
Oct 1998	• FedCIRC officially operational. GSA provides interim funding
Jan 2000	• National Plan for Information Systems Protection
Oct 2000	• Appropriation received funding FY01 FedCIRC operations
Nov 2000	• Government Information Security Reform Act

U. S. General Services Administration
Federal Technology Service

GSA

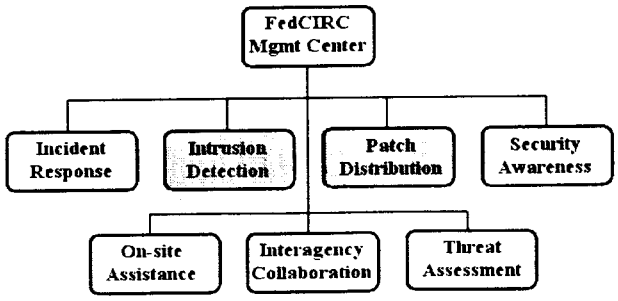
FedCIRC Services

- **Incident Reporting**
  - Telephone Hotline 24X7
  - Electronic Mail
  - Facsimile
- **Information and Security Tools Dissemination**
  - Newsletters
  - Web Page
  - Security Documents
  - Software Security Tools
  - Conference, forum and meeting presentations
- **Security Awareness**
  - Alerts, Advisories and Bulletins
- **Incident Handling**
  - Conduct triage and analysis
  - Containment and recovery assistance, incident correlation and analysis
  - Augment existing agency emergency response capabilities
  - Strategic Defense Planning

U. S. General Services Administration
Federal Technology Service

GSA

FedCIRC Functional Roles



Denotes under development

GSA

FedCIRC's Focus

- **Centralize the collection of reports of unauthorized intrusions, malicious activities and other events impacting critical government service functions**
- **Correlation of security relevant events across government**
- **Collaboration and strategic planning for wide-scale attacks**
- **Preemptive response to prevent or minimize the impact of future incidents**
- **Collaborate with affected agencies, National Security and Law Enforcement activities to assist in investigative actions as situations dictate**

GSA

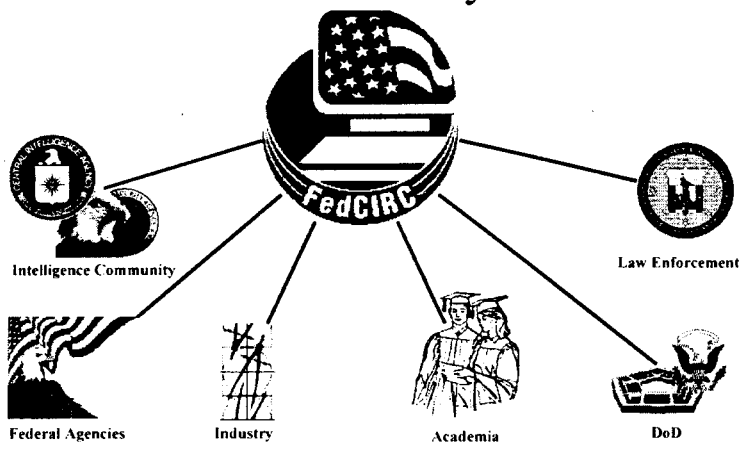
FedCIRC Relationships

Customer Base	All Federal Civilian Agencies and Departments
FedCIRC Partners	NIPC, NSA, FAA, EPA, DARPA, Customs, Energy, NASA, USCG, Senate, HR, DoD CERT, DOS, NIST, USPS, SBA, NSWDD, NLRB, NCUA, MSPB, CPSC, NARA,SSA, GSA, VA, MINT, DOI, NIH, HUD, Education, FERC, JTF-CND, USDA
Critical Incident Coordination	NIST, NSA, NIPC, JTF-CND, DoD CERT, CERT/CC, NSC, OMB, USSS

U. S. General Services Administration
Federal Technology Service

GSA

FedCIRC Collaboration Community



U. S. General Services Administration
Federal Technology Service

FedCIRC Contact Information

For Incident Response:

FedCIRC Operations

Tel: 1-888-282-0870

Fax: 412-268-6989

E-mail: fedcirc@fedcirc.gov

For Information:

FedCIRC Management Center

Tel: 202-708-5060

Fax: 202-318-0899

Email: fedcirc-info@fedcirc.gov

URL: http://www.fedcirc.gov

U. S. General Services Administration
Federal Technology Service

Profiles of Major Incidents

Below are profiles of three major incidents that occurred in 2000 and affected government agencies.

1. T0rn Rootkit

T0rnkit is a collection of files designed to replace portions of the operating system with the intent of providing a more suitable environment to intrude on other computers. It has features that obfuscate this installation, avoid authentication measures, and attack other computers. T0rnkit has been installed on thousands of computers worldwide, including several in US Government agencies. Four agencies have reported rootkit incidents. The extent of any damage from rootkit has not been reported to FedCIRC.

There is some evidence that this rootkit is of foreign origin, and foreign sites remain frequently identified in intrusion reports. The rootkit itself does not markedly interfere with operation of the computer, but it grants unauthorized privilege to intruders. There are multiple styles of intrusion that use this rootkit, showing differing levels of expertise on the part of the intruders, differing language abilities, and differing goals. This appears to be more of a "means to an end" than an end in itself, and as such bears close future examination.

2. Halloween Hack Attack

The "Halloween Hack Attack" was a mass web page defacement, which took place between September 6, 2000 and October 16, 2000. Ten U. S. Government domain web pages were defaced. The defacements were signed and messages were left on the affected web pages. No irreparable damage was done to the compromised machines.

3. Love Letter Malicious Code

"Love Letter" is a malicious program (categorized as a worm) which spreads in a variety of ways. FedCIRC received reports that indicated virtually all government sites suffered some related repercussions. Though many government sites did not propagate the love letter "worm," they still saw marked increase in the amount of incoming mail from external organizations and individuals that employed Microsoft Outlook as their mail client. Several government agencies and departments, in a panic response to the flood of email clogging their systems, chose to disconnect their networks from the Internet. This action did limit the propagation of the worm to some extent but it also prevented agencies from receiving critical information and solutions to the problem. In general, there were numerous reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the "love letter" malicious code.

Department of Health and Human Services

OFFICE OF INSPECTOR GENERAL

REPORT ON THE FINANCIAL STATEMENT AUDIT OF THE DEPARTMENT OF HEALTH AND HUMAN SERVICES FOR FISCAL YEAR 2000

FEBRUARY 2001
A-17-00-00014

INDEPENDENT AUDITOR'S REPORT

INSPECTOR GENERAL'S REPORT ON THE DEPARTMENT OF HEALTH AND HUMAN SERVICES CONSOLIDATED/COMBINED FINANCIAL STATEMENTS FOR FISCAL YEAR 2000

To: The Secretary of Health
and Human Services

We have audited the accompanying consolidated balance sheet of the Department of Health and Human Services (HHS) as of September 30, 2000; the related consolidated statements of net cost and changes in net position; and the combined statements of budgetary resources and financing (principal financial statements) for the fiscal year (FY) then ended. These financial statements are the responsibility of HHS management. Our responsibility is to express an opinion on them based on our audit.

We conducted our audit in accordance with auditing standards generally accepted in the United States; *Government Auditing Standards* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin 01-02, *Audit Requirements for Federal Financial Statements*. These standards require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the principal financial statements referred to above present fairly, in all material respects, the HHS assets, liabilities, and net position at September 30, 2000; the consolidated net costs and changes in net position; and the combined budgetary resources and financing for the year then ended in conformity with accounting principles generally accepted in the United States.

Our audit was conducted for the purpose of forming an opinion on the principal financial statements referred to in the first paragraph. The information in the Overview and the Supplementary Information are not required parts of the principal financial statements but are considered supplemental information required by OMB Bulletin 97-01, *Form and Content of Agency Financial Statements*, as amended. Such information, including trust fund projections,

has not been subjected to the auditing procedures applied in the audit of the principal financial statements. Accordingly, we express no opinion on it.

In accordance with *Government Auditing Standards*, we have also issued our reports dated February 26, 2001, on our consideration of HHS internal controls over financial reporting and on our tests of HHS compliance with certain provisions of laws and regulations. These reports are an integral part of our audit; they should be read in conjunction with this report in considering the results of our audit.

February 26, 2001

REPORT ON INTERNAL CONTROLS

We have audited the principal financial statements of HHS as of and for the year ended September 30, 2000, and have issued our report thereon dated February 26, 2001. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 01-02, *Audit Requirements for Federal Financial Statements*.

In planning and performing our audit, we considered the HHS internal controls over financial reporting by obtaining an understanding of the HHS internal controls, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin 01-02. We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982, such as those controls relevant to ensuring efficient operations. The objective of our audit was not to provide assurance on internal controls. Consequently, we do not provide an opinion on internal controls.

Our consideration of internal controls over financial reporting would not necessarily disclose all matters in these controls that might be reportable conditions. Under standards issued by the American Institute of Certified Public Accountants, reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal controls that, in our judgment, could adversely affect the HHS ability to record, process, summarize, and report financial data consistent with management assertions in the financial statements. Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements in amounts material to the financial statements may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in internal controls, misstatements, losses, or noncompliance may nevertheless occur and not be detected. However, we noted certain matters discussed below involving internal controls and their operation that we consider to be reportable conditions and material weaknesses.

In addition, we considered the HHS internal controls over Required Supplementary Stewardship Information by obtaining an understanding of the HHS internal controls, determining whether these controls had been placed in operation, assessing control risk, and performing tests of controls as required by OMB Bulletin 01-02. Our procedures were not intended to provide assurance on these controls; accordingly, we do not provide an opinion on them.

Finally, with respect to internal controls related to performance measures reported in the *FY 2000 HHS Accountability Report*, we obtained an understanding of the design of significant internal controls related to existence and completeness assertions, as required by OMB Bulletin 01-02. Our procedures were not designed to provide assurance on internal controls over performance measures; accordingly, we do not provide an opinion on such controls.

Using the criteria and standards established by the American Institute of Certified Public Accountants and OMB Bulletin 01-02, we identified two internal control weaknesses that we consider to be material and two reportable conditions, as follows:

INTERNAL CONTROL WEAKNESSES*

		Page
	Material Weaknesses	
1.	Financial Systems and Processes	4
2.	Medicare Electronic Data Processing	13
	Reportable Conditions	
1.	Medicaid Estimated Improper Payments	17
2.	Departmental Electronic Data Processing	18

* "Financial Systems and Processes," called "Financial Systems and Reporting" in our FY 1999 report, has been retitled to incorporate continued problems with Medicare accounts receivable and Health Care Financing Administration oversight of Medicare contractors. The reportable condition for "Property, Plant, and Equipment" has been removed.

MATERIAL WEAKNESSES

1. Financial Systems and Processes (Repeat Condition)

Since passage of the Chief Financial Officers (CFO) Act, as amended by the Government Management Reform Act of 1994, agencies have prepared financial statements for audit by the Inspectors General. The act emphasized production of reliable financial statements; consequently, HHS worked diligently to prepare statements capable of receiving an unqualified audit opinion. With this year's audit, HHS sustained the important achievement of an unqualified, or "clean," opinion, which we issued for the first time on the FY 1999 financial statements.

A clean audit opinion, however, assures only that the financial statements are reliable and fairly presented. The opinion provides no assurance on the effectiveness and efficiency of agency financial controls and systems, criteria for which may be found in OMB Circular A-123, *Management Accountability and Control*, and OMB Circular A-127, *Financial Management Systems*. Taken together, the criteria require agencies to record, classify, and report on the results of transactions accurately and promptly. Although manual processes may be used, the system(s) must be efficient and effective to accomplish the agency mission and to satisfy financial management needs.

In our view, the Department continues to have serious internal control weaknesses in its financial systems and processes for producing financial statements. Because many systems were not fully integrated and, in some cases, were in the process of being updated or replaced, the preparation of financial statements required numerous manual account adjustments involving billions of dollars. In addition, significant analysis by Department staff, as well as outside consultants, was necessary to determine proper balances months after the close of the fiscal year. Had the operating divisions followed departmental policies and conducted financial analyses and reconciliations throughout the year, many account anomalies would have been detected earlier. While we observed steady improvement in the financial statement process, system and process weaknesses still did not ensure the production of timely and reliable financial statements. These weaknesses related to grant and other accounting issues, Medicare accounts receivable, and Health Care Financing Administration (HCFA) oversight of Medicare contractors.

Background

In addition to the individual operating divisions, two divisions of the Program Support Center play important roles in the departmental financial process: the Division of Financial Operations (DFO) and the Division of Payment Management (DPM).

The DFO provides financial management and accounting services to the Administration for Children and Families (ACF), the Substance Abuse and Mental Health Services Administration (SAMHSA), the Health Resources and Services Administration (HRSA), the Indian Health Service, the Administration on Aging, the Program Support Center, the Agency for Healthcare Research and Quality, and the Office of the Secretary. The remaining operating divisions — HCFA, the National Institutes of Health (NIH), the Centers for Disease Control and Prevention (CDC), and the Food and Drug Administration (FDA) — are responsible for their own accounting.

The DPM provides centralized electronic funding and cash management services for approximately 65 percent of Federal civilian grants and certain contracts. In FY 2000, the DPM Payment Management System made almost 274,000 payments totaling approximately

$195 billion to more than 24,000 grantees on behalf of HHS as well as 10 other Federal agencies and 42 subagencies.

After awarding grants, agencies transmit award amounts and grant payment limits to DPM. Based on these parameters, grantees withdraw funds to pay the expenses of their operations, and they report their expenses to DPM quarterly. The DPM records the withdrawals and expenses and issues reports on these transactions to granting agencies and the Department of the Treasury.

Grant Accounting Issues

From 1970 until July 2000, grant transactions were processed by the DPM Payment Management System on a mainframe computer at the NIH Center for Information Technology. In FY 1994, it was determined that expanding this legacy system was not practical and that the system should be replaced with a new client server, web-enabled system. Programming of the new system began in early FY 1998. In February 1999, a decision was made to defer implementation of the new system until after January 2000, and efforts were then focused on remediating the legacy system for Y2K compliance. Independent public accountants (IPAs) determined that for the period September 1, 1999, through July 28, 2000, the legacy system's internal controls were operating effectively. In July 2000, after successfully running parallel for about a month to test the more critical functions, such as fund transfers, the new Payment Management System was brought online without major incident. Grant authorizations, payment requests, and fund transfers were processed through the system at expected volumes.

However, the expenditure subsystem used to produce and process forms 272, Federal Cash Transactions Report, was not fully tested. The DPM determined that this subsystem could be tested after the new system was implemented and before recipients began returning their completed June 30 (third quarter) expenditure reports in September. While processing the June 30 expenditure reports, two programming problems surfaced. As a result, incomplete or erroneous data were reported to the operating divisions and other customer agencies. First, the algorithm used to allocate expenditures to a common accounting number (CAN) did not function properly. While total expenditures were captured, the amounts were incorrectly distributed to the CANs. Although we noted certain concerns with the allocation of disbursements among the operating divisions, we determined that total cash disbursements charged to the operating divisions, in the aggregate, equaled net cash disbursements reported to the Department of the Treasury and distributed to grant recipients. Second, the new system could not process paper 272 reports; this produced a backlog of about $2.1 billion in unprocessed reports. Compounding these problems, the lead programmer working on the expenditure process unexpectedly left the employment of the system development contractor in August.

After correcting the programming problems, DPM began processing the backlog of expenditure reports. In late September, an expenditure file was distributed to the operating divisions reflecting what DPM thought was the majority of grantee expenditure reports. **Because DPM was of the opinion that any remaining expenditure amounts would be immaterial, it did not notify any of its customers of this problem.** These assumptions were incorrect. In actuality, many of the paper 272 reports involved large grantees and totaled about $2.1 billion in unprocessed third quarter expenditures. The DPM should have analyzed the unprocessed reports and determined the extent and seriousness of the problem rather than speculate that it was immaterial. These problems were not fully communicated to senior operating division management or the auditors until February 2001. As a result, grant expenditures, grant advances, and the grant accrued expense calculation contained billions of dollars in errors until final correction. The errors caused account anomalies noted by auditors and substantially delayed final conclusion of the audits of NIH, ACF, HRSA, SAMHSA, and CDC and the Department's compilation of the financial statements:

- The DFO, the operating divisions, and/or auditors analyzed grant expenditures reported on the Statement of Net Cost and found that the yearend balances contained aggregate errors of $2.7 billion. This amount included understatements of $2.1 billion ($1 billion for ACF, $1 billion for NIH, and $100 million for CDC) and overstatements of $628 million ($420 million for HRSA, $97 million for CDC, $91 million for SAMHSA, and $20 million for ACF). As a result of these errors, the financial statements initially were materially misstated. Certain operating divisions did not detect these errors through their internal controls.

- The DFO extensively analyzed July and August grant advance transactions reported by DPM and determined that advances recorded in the general ledger were understated by $858 million: $449 million for ACF, $335 million for HRSA, and $74 million for SAMHSA.

- From October 1, 1999, to June 30, 2000, many accounts in the subsidiary detail were not properly classified as intragovernmental or nongovernmental transactions. The absolute value of classification errors in the subsidiary detail was approximately $6.4 billion: $5.4 billion for ACF, $552 million for HRSA, and $445 million for SAMHSA. The DFO ultimately corrected these errors ("outside the general ledger") in its manual yearend process of preparing financial statements.

- The ACF grant transactions of approximately $1.1 billion were recorded to the wrong CAN. As a result, these amounts were reported in the wrong appropriation. We were informed that this occurred because of discrepancies in

the CAN table that were not identified until several months after the end of the fiscal year.

Although these four problems were eventually corrected, we remain concerned that the operating divisions did not routinely analyze accounts to detect such accounting anomalies. When such analyses are not performed in the normal business cycle, material errors and irregularities will not be promptly detected and the resulting financial statements will be at risk of inaccuracies. Also, procedures should be established to ensure that detected anomalies are effectively communicated to top management.

Medicare Accounts Receivable

The HCFA is the Department's largest operating division with about $316 billion in net outlays. Along with its Medicare contractors, HCFA is responsible for managing and collecting many billions of dollars of accounts receivable each year. Medicare accounts receivable are primarily overpayments owed by health care providers to HCFA and funds due from other entities when Medicare is the secondary payer. For FY 2000, the contractors reported about $30 billion in Medicare accounts receivable activity which resulted in an ending gross balance of approximately $7.1 billion — over 87 percent of HCFA's total receivable balance. After allowing for doubtful accounts, the net balance was about $3.2 billion.

For several years, we have reported serious errors in contractor reporting of accounts receivable that resulted from weak financial management controls. Control weaknesses were noted again this year. Because the claim processing systems used by the contractors lacked general ledger capabilities, obtaining and analyzing financial data was a labor-intensive exercise requiring significant manual input and reconciliations between various systems and ad hoc spreadsheet applications. The lack of double-entry systems and the use of ad hoc supporting schedules increased the risk that contractors could report inconsistent information or that information reported could be incomplete or erroneous.

To address previously identified problems in documenting and accurately reporting accounts receivable, HCFA began a substantial validation of its receivables by contracting with IPAs in FY 1999. The HCFA continued the validation effort this year. As a result, the receivables balance was adequately supported as of the end of FY 2000.

The IPAs reviewed accounts receivable activity at 14 Medicare contractors which represented over 68 percent of the total Medicare accounts receivable balance at September 30, 1999. While they noted significant improvement in the HCFA central office's analysis of information included in its financial statements, along with improvement in contractors' processing and reporting of receivables, their review identified overstatements and understatements totaling

$374 million as of March 31, 2000. This amount included errors of $201 million in Medicare Secondary Payer (MSP) receivables and $173 million in non-MSP receivables. Most of the MSP misstatements were due to a lack of supporting documentation for the amounts reported in the contractors' quarterly financial reports to HCFA. Misstatements of non-MSP receivables were attributed to the following:

- $74 million resulted from clerical and other errors.
- $50 million should have been eliminated when providers eventually filed their cost reports. Until a provider files a cost report, all outstanding interim payments are considered technical overpayments and are recorded as receivables.
- $47 million was not supported by records.
- $2 million concerned receivables transferred to a HCFA regional office but still included on the contractor's books and thus recorded twice.

While it is quite clear that the root cause of the accounts receivable problem is the lack of an integrated, dual-entry accounting system, HCFA and the Medicare contractors have not provided adequate oversight or implemented compensating internal controls to ensure that receivables will be properly accounted for and reflected in their financial reports. To address its systems problem, HCFA plans to develop a state-of-the-art Integrated General Ledger Accounting System. This system will replace the cumbersome, ad hoc spreadsheets currently used to accumulate and report contractor financial information and will enable HCFA to collect standardized accounting data. In addition, the system will replace HCFA's current accounting system, the Financial Accounting Control System, and will include an accounts receivable module to provide better control and support for receivables. A HCFA-wide project team has been formed under the guidance of the CFO and the Chief Information Officer. Depending on funding, HCFA does not expect to implement the new system until FY 2007.

HCFA Oversight of Medicare Contractors

Pending implementation of a fully integrated accounting system, HCFA's oversight of the Medicare contractors becomes critical to reducing the risk of material misstatement in the financial statements. However, as discussed below, HCFA oversight of contractor operations and financial management controls has not provided reasonable assurance that material errors will be detected in a timely manner.

The responsibility for collecting delinquent provider overpayments is dispersed among the 54 Medicare contractors, the 10 HCFA regional offices, the HCFA central office, and external

agencies. The majority of overpayments are recovered by the contractors through offset procedures. However, when the contractors' collection efforts are unsuccessful, delinquent receivables are transferred to the regional offices and then possibly to various other locations, including the central office, the HCFA Office of General Counsel, the Department of Justice, and the Department of the Treasury's Debt Collection Center.

In an October 28, 1999, report to HCFA (*Safeguarding Medicare Accounts Receivable*, A-17-99-11999), we noted significant weaknesses in regional office accounting for debt. Our review showed that regional and central office accounts receivable were misstated by $184.5 million. Examples of the misstatements included:

- an overstatement of $96.9 million in receivables with no supporting documentation,
- overstatements and understatements totaling $33.9 million due to various reporting and clerical errors, and
- an understatement of $21 million in improperly recorded transfers of receivables from the Medicare contractors to the regional offices.

Not only did the regional offices not safeguard debt in their custody, their monitoring of contractor financial information was inadequate to prevent errors in financial reports and data. As mentioned above, it was necessary for HCFA to hire IPAs to properly determine the accounts receivable balance for the past 2 years. For non-MSP receivables during this period, the IPAs identified about $590 million in recorded debt that the Medicare contractors could not support. While these receivables were written off because of the lack of support, it is possible that some of these receivables were actually debt due to Medicare and should have been collected. Had the regional offices been required to conduct reviews similar to those conducted by the IPAs, many of these problems could have been detected or prevented more timely.

Similarly, stronger regional office oversight of the contractors' reconciliations would help to ensure that contractors have adequate controls in place to prepare accurate and complete financial reports. The HCFA requires all Medicare contractors to reconcile "total funds expended" reported on the prior month's HCFA 1522, Monthly Contractor Financial Report, to adjudicated claims processed using the paid claims tape. This reconciliation is an important control to ensure that all amounts reported to HCFA by Medicare contractors are accurate, supported, complete, and properly classified. However, of the 10 contractors in our sample, 9 did not conduct this reconciliation using the actual paid claims tape. Numerous errors and omissions in contractor reporting resulted. For example, at one contractor, over $65 million in paid claims from the current month's HCFA 1522 was inadvertently included in the previous month's HCFA 1522.

The contractor's HCFA 1522 had to be resubmitted because an unreported manual payment of $6.3 million had not been posted to the contractor's financial records.

Other Accounting Issues

While the timeliness of the HHS financial statements has improved, delays were noted again this year. Numerous adjusting entries at yearend were needed to correct errors and to develop accurate financial statements. Many of these adjustments would not have been necessary had management routinely reconciled and analyzed accounts throughout the year, recorded transactions using prescribed accounts, and refrained from making "financial statement only" adjustments. These controls help to promptly identify and correct accounting aberrations, provide more reliable financial information during the year, and prevent a material misstatement of the financial statements at yearend. Some examples follow:

National Institutes of Health. The NIH financial system, which dates back to the early 1970s, was not designed for financial reporting purposes and lacks certain system interfaces. Because the accounting function is decentralized among the 25 NIH Institutes and Centers, the NIH Office of Financial Management spent considerable time in consolidating and adjusting 23 trial balances in order to prepare financial statements. The NIH, which had net budget outlays of $15.4 billion, was unable to prepare reliable financial statements for September 30, 2000, until February 2001.

During FY 2000, NIH recorded approximately 9.4 million entries in its financial system. About 18,000 of these entries, with an absolute value of about $200 billion, were recorded using nonstandard accounting entries which could circumvent accounting controls. The bulk of these transactions pertained to FY 1999 manual closing entries. Many of these entries were incorrect and were not corrected until months after the original transactions were recorded. For example, entries totaling $140 million were recorded three times in April 2000. Four months later, the duplicate entries were reversed, leaving the correct entries in the system. In addition, we noted that NIH, as in past years, delayed entering some of the prior year's financial statement adjustments, valued at $5.1 billion, to its general ledger for nearly a full year. Such delays cause the general ledger to be misleading and inaccurate during the year.

For FY 2000, to compensate for system inadequacies, NIH developed an ad hoc, yearend process to create and post correct standard general ledger accounts. The output of this process formed the trial balance. However, an additional 95 entries, totaling an absolute value of approximately $28 billion, were necessary in order to adjust the trial balance to prepare the financial statements.

In 1998, NIH launched a project known as the NIH Business System to replace existing administrative and management systems. Once the new system is fully implemented, we believe

that improved financial information will provide for better decision-making, potential cost savings, and a means to meet current Federal accounting and budgetary reporting requirements. However, the system is not expected to be fully operational until 2005.

Administration for Children and Families. The ACF, the second largest operating division with net budget outlays of $37.5 billion, prepared its financial statements more accurately and more timely than last year, largely as a result of having performed many of the required reconciliations and analyses during the year. But many "Fund Balance with Treasury" reconciliations were performed late, and most of the required budgetary account reconciliations were not performed until yearend to prepare the financial statements.

Fund Balance with Treasury reconciliations deserve particular mention because the differences between the general ledger and the Department of the Treasury's records were so great. At various times, the difference ranged from $200 million to $6.3 billion. This suggests that ACF did not post transactions timely or accurately; in our testing, we found instances of this problem. For example, we noted that a $143 million transaction had been posted to the wrong appropriation and remained uncorrected for over a year.

Recommendations. We recommend that the Assistant Secretary for Management and Budget (ASMB):

- direct each operating division to establish controls to identify and report significant accounting anomalies to top management;
- direct the CFO of the Program Support Center to communicate accounting and control problems more effectively to the CFOs of serviced entities;
- direct that operating division CFOs work with their program office counterparts to develop procedures for analyzing and explaining unusual changes in account balances;
- oversee and maintain close liaison with entities serviced by the Program Support Center and CFO offices during the installation of new systems or the revision of operating procedures;
- continue to support the development of the HCFA Integrated General Ledger Accounting System and oversee its implementation;

- monitor HCFA's corrective actions to strengthen regional office and contractor monitoring of accounts receivable and to ensure that key financial reconciliations are performed timely;

- consider directing operating division CFOs to prepare and analyze interim financial statements, particularly the statements of net cost, budgetary resources, and financing, as an aid in the reconciliation and analysis process; and

- require each operating division to prepare quarterly reports on the status of corrective actions on recommendations in the specific CFO reports on internal controls. The ASMB, in turn, should summarize and report quarterly on these actions to the Deputy Secretary and OIG.

2. Medicare Electronic Data Processing (Repeat Condition)

The HCFA relies on extensive electronic data processing (EDP) operations at both its central office and Medicare contractor sites to administer the Medicare program and to process and account for Medicare expenditures. Internal controls over these operations are essential to ensure the integrity, confidentiality, and reliability of critical data while reducing the risk of errors, fraud, and other illegal acts.

The HCFA central office systems maintain administrative data, such as Medicare enrollment, eligibility, and paid claims data, and process all payments for managed care. In FY 2000, managed care payments totaled about $39.8 billion. The Medicare contractors and data centers use several "shared" systems to process and pay fee-for-service claims. All of the shared systems interface with HCFA's Common Working File (CWF) to obtain authorization to pay claims and to coordinate Medicare Part A and Part B benefits. This network accounted for and processed $173.6 billion in Medicare expenditures during FY 2000.

Our review of EDP internal controls covered general and application controls. General controls involve the entity-wide security program, access controls, application development and program change controls, segregation of duties, operating system software, and service continuity. General controls affect the integrity of all applications operating within a single data processing facility and are critical to ensuring the reliability, confidentiality, and availability of HCFA data. Application controls involve input, processing, and output controls related to specific EDP applications.

We completed general control reviews at nine Medicare data processing facilities that support the Medicare contractors sampled. In addition, we assessed application controls of the Fiscal Intermediary Shared System (FISS), the Multi-Carrier System, and the CWF at three separate

contractors. At the HCFA central office, we updated the status of prior-year findings concerning general controls.

We found numerous EDP general control weaknesses, primarily at the Medicare contractors. Such weaknesses do not effectively prevent (1) unauthorized access to and disclosure of sensitive information, (2) malicious changes that could interrupt data processing or destroy data files, (3) improper Medicare payments, or (4) disruption of critical operations. Further, weaknesses in the contractors' entity-wide security structure do not ensure that EDP controls are adequate and operating effectively.

As noted in the following table, a total of 124 weaknesses were identified. The majority were found at the Medicare contractors, and most (about 80 percent) involved three types of controls: access controls, entity-wide security programs, and systems software. While individually the conditions found are not material, the cumulative effect is material.

General Control Audit Areas	Number of Weaknesses		Total
	Central Office	Medicare Contractors	
Access controls	2	55	57
Entity-wide security programs	4	17	21
Systems software	1	20	21
Service continuity/contingency planning	-	11	11
Segregation of duties	1	7	8
Application software development and change controls	1	5	6
Total	**9**	**115**	**124**

Access controls. Access controls ensure that critical systems assets are physically safeguarded and that logical access to sensitive computer programs and data is granted only when authorized and appropriate. Closely related to these controls are those over computer operating systems and data communications software. These controls further ensure that only authorized staff and computer processes access sensitive data in an appropriate manner. Weaknesses in such controls can compromise the integrity of sensitive program data and increase the risk that such data may be inappropriately used and/or disclosed. However, access control weaknesses represented the largest problem area. Of the 124 EDP control weaknesses reported, 57, or 46 percent, related to access controls.

- ***Administration of access controls*** (29 conditions: 27 at 11 Medicare contractor sites and 2 at the HCFA central office). In numerous instances, passwords were not properly administered, systems security software was not implemented effectively, or access privileges were not reviewed frequently enough to ensure their continuing validity.

- ***Access to computer programs and system files*** (5 conditions at 5 Medicare contractor sites). At some sites, installation-level controls over critical system software libraries were inadequate, and programmers were inappropriately allowed access to production software program libraries. We also noted cases in which programmers had inappropriate access to system logs; this provided an opportunity to conceal improper actions and obviated the logs' effectiveness as a detect control. At another site, the computer operator could override installation system security precautions when restarting the mainframe computer system.

- ***Access to sensitive data*** (15 conditions at 9 Medicare contractor sites). These are instances in which computer programmers and/or other technical support staff had inappropriate access to the data files used in the claim process. At several sites, programmers had inappropriate access to beneficiary history files. Under these conditions, the CWF system was vulnerable to inappropriate use. At several other sites, programmers had inappropriate access rights to production files, including beneficiary history and other sensitive data. Also, users of one contractor's local area network could access Medicare program data without adequate controls. During vulnerability testing at three Medicare contractor sites, excessive remote access attempts were permitted and more information about the computers being tested was disclosed than necessary. Such weaknesses increase the risk of unauthorized remote access to sensitive Medicare systems.

- ***Physical access*** (8 conditions at 5 Medicare contractor sites). These include weaknesses in controls over access to sensitive facilities and media within those facilities. For example, at one contractor, inappropriate individuals had access to the computer center's command post. At another, the computer production control area was not secured during normal business hours.

Entity-wide security programs. These programs are intended to ensure that security threats are identified, risks are assessed, control objectives are formulated, control techniques are developed, and management oversight is applied to ensure the overall effectiveness of security measures. Programs typically include policies on how and which sensitive duties should be separated to avoid conflicts of interest. Likewise, policies on background checks during the hiring process are usually stipulated. Entity-wide security programs afford management the opportunity to

provide appropriate direction and oversight of the design, development, and operation of critical systems controls. Inadequacies in these programs can result in inadequate access controls and software change controls affecting mission-critical, computer-based operations. Of the 124 EDP control weaknesses reported, 21, or 17 percent, related to security program weaknesses.

- ***Entity-wide plans*** (8 conditions at 8 Medicare contractor sites). Eight contractor sites lacked fully documented, comprehensive entity-wide security plans that addressed all aspects of an adequate security program. One site also had no mechanism for ensuring that system audit findings were effectively addressed and resolved.

- ***Implementation of entity-wide plans*** (13 conditions: 9 at 6 Medicare contractor sites and 4 at the HCFA central office). Inadequate risk assessments, a lack of comprehensive security awareness programs, and inadequate policies were among the weaknesses reported at the contractors. At the HCFA central office, four conditions remained reportable: no security assessment of, or security plans for, significant application systems; deficiencies in the security plan accreditation process; insufficient security oversight of the Medicare contractors; and no formal process to remove system access of terminated HCFA employees and contractors.

Systems software controls. Systems software is a set of programs designed to operate and control the processing activities of computer equipment. Generally, it is used to support and control a variety of applications that may run on the same computer hardware. Systems software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on a system. Some systems software can change data and programs on files without leaving an audit trail. Of the 124 EDP control weaknesses, 21, or 17 percent, related to weaknesses in systems software controls (20 at 7 Medicare contractor locations and 1 at the HCFA central office). Problems related to managing routine changes to systems software to ensure their appropriate implementation and configuring controls associated with the operating system to ensure their effectiveness. Such problems could weaken critical controls over access to sensitive Medicare data files and operating system programs.

Shared system weaknesses. We found that the prior control weakness related to the Medicare data centers' having full access to the FISS source code remained unresolved. This weakness has been expanded to include the CWF system, since the design of the CWF software provides for programmer update access to CWF data files to meet operational needs. As we previously reported, Medicare data centers had access to the FISS source code and were able to implement local changes to FISS programs. Such access may be abused, resulting in the implementation and processing of unauthorized programs at contractor data centers. While HCFA requires

contractors to restrict local changes to emergency situations, local changes are often not subjected to the same controls that exist in the standard change control process.

HCFA central office. Our followup work found that the HCFA central office had resolved the prior-year deficiency in mainframe database access controls. The central office has also continued to implement enhanced control procedures, specifically in access controls and application development and program change controls. However, actions were still underway as of the end of FY 2000. Improvements not yet completed included:

- issuance of task orders to various contractors to address issues related to risk assessment, security policies and procedures, independent verification and validation of entity-wide security plans, and related procedures for significant systems and
- migration to enterprise-wide program change management software, with full implementation planned during FY 2001.

Recommendation. We recommend that ASMB oversee HCFA's identification and implementation of corrective actions to address the fundamental causes of Medicare EDP control weaknesses. Detailed recommendations are contained in the HCFA audit report.

REPORTABLE CONDITIONS

1. Medicaid Estimated Improper Payments (Repeat Condition)

The Medicaid program, enacted in 1965 under Title XIX of the Social Security Act, is a grant-in-aid medical assistance program largely for the poor, the disabled, and persons with developmental disabilities requiring long-term care. Funded by Federal and State dollars, the program is administered by HCFA in partnership with the States via approved State plans. Under these plans, States reimburse providers for medical assistance to eligible individuals, who numbered more than 33 million in 2000. In FY 2000, Federal and State Medicaid outlays totaled $207.1 billion; Federal expenses were $118.7 billion.

We found that HCFA still lacked a methodology to estimate the extent of improper Medicaid payments on a national level. For the last 5 years, OIG reviewed a statistical sample of Medicare claims and estimated the extent of payments that did not comply with laws and regulations. The majority of errors fell into four broad categories: unsupported services, medically unnecessary services, incorrect coding, and noncovered services. This information helped HCFA to monitor and reduce improper Medicare payments. Because HCFA has not established a similar methodology for the Medicaid program, it cannot reach conclusions on the extent of Medicaid

payment errors. We recognize that Medicaid is a State-administered program, so estimates of improper payments will require the cooperation of States.

Our prior report recommended that HCFA work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments. We noted some recent progress in this area. A project coordinator has begun requesting State participation in a pilot error rate project.

Recommendation. We recommend that ASMB and HCFA continue to work with the States to develop procedures and implement a methodology for determining the extent of improper Medicaid payments.

2. Departmental Electronic Data Processing (Repeat Condition)

The following summarizes some of the systemic EDP control weaknesses identified in audits of operating division financial statements and service organization operations. Other weaknesses are reported in the individual reports on these entities. We note that NIH has resolved the previous year's reportable findings related to systems access controls.

Division of Financial Operations. The Program Support Center's DFO uses several automated systems to provide financial services to certain operating divisions. While DFO continues to strengthen controls over these systems, further improvements are needed.

- The DFO entity-wide security program lacked a formal risk assessment, a formal security plan, and adequate personnel security policies. In addition, the security features of the DFO accounting system (CORE) were not accredited as required by OMB Circular A-130. Such weaknesses in the entity-wide security structure limited assurance that EDP controls were adequate and operating effectively.

- The DFO policy for application change control included no formal test procedures and lacked adequate emergency change procedures, as well as adequate library management software. Additionally, DFO did not consistently follow its documented application change control procedures. For example, change request forms, used to ensure that software changes are approved and documented, were not always complete; supervisory approval of program modifications was not consistently documented; and "before and after" images of program code were not compared to ensure that only approved changes were made to the CORE application.

- A penetration test of the DFO internal network and computing resources to assess the security of systems and to identify vulnerabilities determined that user account policies and administrative passwords on servers were weak. This type of weakness increases to a high level the risk that the system will be compromised by unauthorized users.

Food and Drug Administration. In FY 1999, FDA had several findings under each of the six major categories of general controls. Although FDA resolved many of these findings, some were still outstanding this year. When viewed in the aggregate, these exceptions constituted a reportable condition. Areas still in need of improvement included the entity-wide security program, access controls, software application change controls, and service continuity.

Recommendation. We recommend that ASMB oversee the efforts of the operating divisions and service organizations to improve security issues, system access controls, application change controls, and service continuity plans. Specific recommendations are covered in the individual audit reports.

OTHER MATTERS

FMFIA Reporting

As part of our audit, we also obtained an understanding of management's process for evaluating and reporting on internal control and accounting systems, as required by the Federal Managers' Financial Integrity Act (FMFIA), and compared the material weaknesses reported in the HHS FY 2000 FMFIA report relating to the financial statements under audit with the material weaknesses noted in our report on internal controls. Under OMB guidelines for FMFIA reporting, HHS reports as a material weakness any deficiency the Secretary determines to be significant enough to be disclosed outside the agency. This designation requires HHS management to judge the relative risk and significance of deficiencies. In making this judgment, HHS management pays particular attention to the views of the HHS Inspector General. The HHS management agrees with the HHS Inspector General in reporting to the President and the Congress the two material weaknesses described in this report.

Medicare National Error Rate

At HCFA's request, we developed a national error rate of the extent of improper Medicare fee-for-service payments for FY 2000. As discussed in detail in our separate report (CIN: A-17-00-02000), and based on our statistical sample, we estimate that improper Medicare benefit payments made during FY 2000 totaled $11.9 billion, or about 6.8 percent of the $173.6 billion

in processed fee-for-service payments reported by HCFA. This year's estimate of improper payments is the lowest estimate to date and about half the $23.2 billion that we estimated for FY 1996. There is convincing evidence that this reduction is statistically significant. However, we cannot conclude that this year's estimate is statistically different from the estimates for FY 1999 ($13.5 billion) or 1998 ($12.6 billion). The decrease this year may be due to sampling variability; that is, selecting different claims with different dollar values and errors will inevitably produce a different estimate of improper payments.

As in past years, these improper payments could range from inadvertent mistakes to outright fraud and abuse. We cannot quantify what portion of the error rate is attributable to fraud. The overwhelming majority (92 percent) of these improper payments were detected through medical record reviews coordinated by OIG. When these claims were submitted for payment to Medicare contractors, they contained no visible errors. Although HCFA has made substantial progress since FY 1996 in reducing improper payments in the Medicare program, continued efforts are needed.

****

This report is intended solely for the information and use of HHS management, OMB, and the Congress and is not intended to be and should not be used by anyone other than these specified parties.

February 26, 2001

REPORT ON COMPLIANCE WITH LAWS AND REGULATIONS

We have audited the principal financial statements of HHS as of and for the year ended September 30, 2000, and have issued our report thereon dated February 26, 2001. We conducted our audit in accordance with auditing standards generally accepted in the United States; the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States; and OMB Bulletin 01-02, *Audit Requirements for Federal Financial Statements*.

The HHS management is responsible for complying with applicable laws and regulations. As part of obtaining reasonable assurance about whether the HHS financial statements are free of material misstatement, we performed tests of management compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of financial statement amounts, and with certain other laws and regulations specified in OMB Bulletin 01-02, including the requirements referred to in the Federal Financial Management Improvement Act (FFMIA) of 1996.

The results of our tests of compliance with laws and regulations described in the preceding paragraph, exclusive of FFMIA, disclosed no instances of noncompliance required to be reported under *Government Auditing Standards* or OMB Bulletin 01-02.

Under FFMIA, we are required to report whether HHS financial management systems substantially comply with Federal financial management systems requirements, applicable Federal accounting standards, and the United States Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA section 803(a) requirements. The results of our tests disclosed instances, described below, in which HHS financial management systems did not substantially comply with Federal financial management system requirements.

- The financial management systems and processes used by HHS and the operating divisions were not adequate to prepare reliable, timely financial statements. Because the Department is decentralized, operating divisions must have efficient and effective systems and processes to report financial results.
    - At HCFA, extensive consultant support was needed to establish reliable accounts receivable balances and to oversee Medicare contractors.
    - The Payment Management System, an application for processing grant payments, did not record and report grant transactions properly.

- At most operating divisions, suitable systems were not in place to adequately explain significant fluctuations in grant transactions.

- At NIH, an integrated accounting system was not in place to consolidate the accounting results of transactions by the Institutes. Extensive, time-consuming manual adjustments were needed before reliable financial statements could be prepared.

❑ The EDP internal control weaknesses identified at the sampled Medicare contractors were significant departures from requirements in OMB Circulars A-127, *Financial Management Systems*, and A-130, *Management of Federal Information Resources*.

The results of our tests disclosed no instances in which the HHS financial management systems did not substantially comply with applicable Federal accounting standards or the U.S. Government Standard General Ledger.

The HHS CFO prepared a 5-year plan to address FFMIA and other financial management issues. Although certain milestone dates have passed, we recognize that the plan will require periodic updating to reflect changed priorities and available resources.

Providing an opinion on compliance with certain provisions of laws and regulations was not an objective of our audit; accordingly, we do not express such an opinion.

****

This report is intended solely for the information and use of HHS management, OMB, and the Congress. It is not intended to be and should not be used by anyone other than these specified parties.

Michael Mangano

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services

February 26, 2001
CIN: A-17-00-00014

FISCAL YEAR 2000 CFO REPORTS ON HHS OPERATING DIVISIONS AND SERVICE ORGANIZATIONS

Nine separate financial statement audits of HHS operating divisions were conducted in FY 2000:

- Administration for Children and Families *(CIN: A-17-00-00001)*
- Centers for Disease Control and Prevention *(CIN: A-17-00-00008)*
- Food and Drug Administration *(CIN: A-17-00-00006)*
- Health Care Financing Administration *(CIN: A-17-00-02001)*
- Health Resources and Services Administration *(CIN: A-17-00-00003)*
- Indian Health Service *(CIN: A-17-00-00004)*
- National Institutes of Health *(CIN: A-17-00-00007)*
- Program Support Center *(CIN: A-17-00-00005)*
- Substance Abuse and Mental Health Services Administration *(CIN: A-17-00-00002)*

Four Statement on Auditing Standards 70 examinations were conducted:

- Center for Information Technology, NIH *(CIN: A-17-00-00010)*
- Central Payroll and Personnel System, Program Support Center *(CIN: A-17-00-00012)*
- Division of Financial Operations, Program Support Center *(CIN: A-17-00-00009)*
- Payment Management System, Program Support Center *(CIN: A-17-00-00011)*

Appendix II

DEPARTMENT OF HEALTH & HUMAN SERVICES

Office of the Secretary

Washington, D.C. 20201

FEB 26 2001

Michael F. Mangano
Acting Inspector General
Department of Health and Human Services
Washington, D.C. 20201

Dear Mr. Mangano:

This letter responds to the Office of Inspector General opinion of the FY 2000 audited financial statements of the Department of Health and Human Services. We concur with your findings and recommendations.

We are tremendously pleased that, once again, your report reflects an unqualified, or "clean", audit opinion for the Department. Through our joint efforts, we were able to reach the goal of both a clean and timely Departmental financial statement audit.

We also acknowledge that significant internal control weaknesses remain. In addition to the incremental progress we have made on these weaknesses over the last year, we have greatly accelerated our efforts to improve our financial systems to ultimately resolve these material weaknesses.

I would like to thank your office for its continuing professionalism during the course of the audit.

Sincerely,

Dennis P. Williams
Acting Assistant Secretary for Management and Budget/Chief Financial Officer

PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY

March 21, 2001

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
Old Executive Office Building
Washington, D.C. 20503

Dear Mr. Daniels:

This letter presents the Phase I results of a four-phase President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) review of Federal agencies' implementation of Presidential Decision Directive (PDD) 63 related to critical infrastructure protection. The National Aeronautics and Space Administration (NASA), Office of Inspector General (OIG), led the review that included participation of a total of 21 OIGs. All participants either have or will be issuing individual reports to their respective departments or agencies.[1]

Based on the Phase I review results, we are providing our observations and suggestions for strengthening the Federal Government's compliance with PDD 63. The review identified several key areas where improvements can enhance the security of our nation's critical infrastructures.

Background

When signed on May 22, 1998, PDD 63 called for a national effort to assure the security of the nation's critical infrastructures.[2] Under the Directive, the President intends that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on the nation's critical infrastructures, especially its cyber systems. By May 22, 2003, the United States shall have achieved and shall maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services; and

[1] Departments and agencies are hereafter referred to as agencies.
[2] PDD 63 defines critical infrastructure as ". . . those physical and cyber-based systems essential to the minimum operations of the economy and government." Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and essential government services.

- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

Various laws and regulations have addressed the need to secure our nation's key cyber systems including the Government Information Security Reform Act; the Clinger-Cohen Act; the Computer Security Act; and Appendix III to Office of Management and Budget (OMB) Circular A-130, "Security of Federal Automated Information Resources." PDD 63 complements and expands on those laws and regulations by requiring an independent review of security plans for protecting the nation's critical systems; the identification of minimum essential infrastructure (MEI)[3] critical to the operations of the economy and government, including infrastructure interdependencies; and the assessment of MEI vulnerabilities.

On November 17, 1999, the PCIE and ECIE formed a working group to review the Federal agencies' implementation of PDD 63.

Objectives, Scope, and Methodology

Our overall objective was to review the adequacy of the Federal Government's critical infrastructure protection (CIP) program in the context of PDD 63 requirements. The review consists of four phases. Phase I relates to planning and assessment activities for cyber-based infrastructures; Phase II, implementation activities for cyber-based infrastructures; Phase III, planning and assessment activities for physical minimum essential infrastructures; and Phase IV, implementation activities for the physical minimum essential infrastructures. Participating OIGs were responsible for (1) determining the scope of their reviews, (2) performing review work at their respective agencies, and (3) providing the PCIE/ECIE Working Group with a summary of their review results. Also, the Working Group reviewed the coordination activities of the Federal organizations primarily responsible for implementing PDD 63. The 21 OIGs that participated in the Phase I Review are listed in the Enclosure.

In Phase I, the participating OIGs reviewed the adequacy of agency cyber-based plans, asset identification efforts, and initial vulnerability assessments. Specifically, the OIGs determined whether agencies had:

- developed effective plans for protecting their critical cyber-based infrastructures;
- identified their cyber-based MEI and interdependencies; and
- identified the threats, vulnerabilities, and potential magnitude of harm to their cyber-based MEI that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of their critical cyber-based infrastructure investments, and developed remediation plans to address the risks identified.

[3] The Critical Infrastructure Assurance Office (CIAO) has defined agency MEI as "the framework of critical organizations, personnel, systems, and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services."

Overall Review Results

The Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. Specifically, the review determined that:

- Many agency infrastructure plans were incomplete.
- Most agencies had not identified their mission-essential infrastructure assets.
- Almost none of the agencies had completed vulnerability assessments of their MEI assets or developed remediation plans.

When all participating OIGs complete their Phase I Reviews, they will have made an estimated 100 recommendations to improve their respective agency's CIP program.

The OIG reports issued to date present findings that, collectively, question the Federal Government's ability to achieve full operating capability by May 22, 2003, as required by PDD 63. Key factors impacting the agencies' ability to implement PDD 63 are:

- Misunderstanding as to the applicability of PDD 63.
- Imprecise performance measures.
- Untimely identification of critical infrastructures.
- Lack of coordinated management of PDD 63 requirements
- Failure to advance beyond the planning phase.

Each of these factors is discussed below.

Applicability of PDD 63

Several agencies decided to not implement PDD 63 because they believed they were exempt from the Directive. They based their decision on the mistaken belief that PDD 63 applied only to the 19 agencies listed in the Directive and its addendum. As a result, agencies considering themselves exempt from PDD 63 had not prepared the required CIP plans, identified their MEI assets, performed vulnerability assessments of their MEI assets, or developed remediation plans. Most of them have now initiated work to address PDD 63 requirements as a result of our review.

The Director, National Critical Infrastructure Assurance Office (CIAO),[4] told PCIE/ECIE Working Group members that all agencies are subject to PDD 63. The Director highlighted two key criteria in PDD 63 to support his position.

[4] The National Critical Infrastructure Assurance Office supports the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism in developing an integrated national infrastructure assurance plan to address threats to the nation's critical infrastructures. The CIAO also coordinates a national education and awareness program, as well as legislative and public affairs initiatives.

> Section VII: Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems . . . Every department and agency shall appoint a Chief Infrastructure Assurance Officer . . . who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure.
>
> Section V: The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

Much of the confusion regarding the applicability of PDD 63 can be attributed to the Federal Sector Liaison[5] for PDD 63 who told representatives of the agencies not listed in the Directive, that nonlisted agencies were exempt from PDD 63 because they were not specifically identified in the Directive.[6]

We suggest that the Director, Office of Management and Budget, and the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council, direct the National CIAO to advise all Federal agencies of their responsibilities for implementing PDD 63.

Performance Measures

Agencies were required to achieve a level of security preparedness (referred to as initial operating capability (IOC)), not later than December 31, 2000, but had not been advised of the requirements for achieving IOC. Neither the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (who authored the term) nor the Director, National CIAO, had defined IOC. Without a formal definition, achievement of IOC is not a consistent measure of progress toward achieving full security preparedness.

Because the term IOC has not been defined, agencies have used various interpretations. For example, one agency defined IOC to mean "completion of those initial mediation measures that are identified as needed by that time during the vulnerability assessment/mitigation planning process." Representatives responsible for implementing PDD 63 in that agency said they could not understand the agency's definition of IOC. Another agency defined IOC as: "(1) a broad level assessment of MEI should be completed, (2) remediation plans should be completed for assets considered to be the most at risk, and (3) fixes should be in place for the most vulnerable assets."

Although the date for achieving IOC has passed, agencies still need guidance for measuring their progress in completing the identification of critical infrastructure assets, performing vulnerability assessments, developing remediation plans, and implementing the remediation plans. Until such guidance is established, the government continues to lack the visibility needed to accurately assess the status of its infrastructure protection program.

---

[5] The Federal Sector Liaison is located at the General Services Administration.
[6] The Federal Sector Liaison confirmed his interpretation of the scope of PDD 63 to the NASA OIG.

We suggest that the Director, Office of Management and Budget, and the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council, provide guidance that agencies can use to measure their progress in achieving full operating capability.

Identification of Critical Infrastructure

Most of the agencies having CIP plans had not identified or adequately identified their critical, cyber infrastructure assets.[7] The National CIAO has established an asset identification initiative (Project Matrix, discussed below) that agencies can use to identify their critical assets. Unfortunately, the initiative may end before most agencies have had an opportunity to participate in it. Without an accurate and complete inventory of critical assets, agencies cannot identify and remediate their security-related vulnerabilities.

In a July 19, 2000, memorandum, the National Coordinator announced a standardized process, to be administered by the National CIAO, for identifying critical infrastructure assets initially at 14 agencies. The process, called Project Matrix, would:

> . . . identify all assets, nodes and 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 this context, the word "critical" refers to those responsibilities, assets, nodes and networks that if incapacitated or destroyed would: jeopardize the nation's survival; have a serious, deleterious effect on the nation at large; adversely affect large portions of the American populace, and require near-term, if not immediate, remediation.

The Project Matrix team is composed of employees from various agencies and disciplines whose goal is to apply a standard methodology and criteria for helping agencies identify their critical assets.

Although Project Matrix provides a rational and consistent approach for identifying critical infrastructure assets, its success will be diminished by the amount of time needed to implement the process and by the National CIAO's limited time left as a functioning office. Specifically, the Project Manager for Project Matrix stated that the Project Matrix team can review only six to eight agencies a year. In view of the much larger number of agencies that may have critical infrastructure assets, several years would be needed to review all assets. Further, Congress has authorized the National CIAO to function only through September 30, 2001. Without continued funding of the National CIAO, the future of Project Matrix is questionable.

We suggest that the Director, Office of Management and Budget, continue a matrix-like approach for the identification of critical infrastructures for all agencies that may possess them.

---

[7] This condition occurred for a variety of reasons including the lack of funds, poor methodology for identifying assets, and higher priority work.

Management of PDD Activities

The organizations primarily responsible for implementing PDD 63 have not effectively coordinated and managed their PDD 63 activities. This condition occurred largely due to the decentralized oversight and responsibilities of the entities implementing PDD 63. As a result, the Federal Government's ability to achieve full operational capability by May 2003, as required by PDD 63, is questionable.

The following organizations are among those responsible for coordinating and/or managing implementation of PDD 63:

- The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism is responsible for coordinating and implementing the Directive. The National Coordinator cannot direct Departments and Agencies but will ensure interagency coordination for policy development and implementation.
- The Office of Management and Budget is responsible for developing information security policies and overseeing agency practices.
- The National Institute of Standards and Technology is responsible for developing technical standards and providing related guidance for sensitive data.
- The National Security Agency is responsible for setting information security standards for national security agencies.
- The National CIAO, an interagency office, is responsible for developing an integrated National Infrastructure Assurance Plan to address threats to the Nation's critical infrastructures.
- The General Services Administration (GSA) is the designated lead agency for the Federal sector.

The absence of coordinated oversight and management of PDD 63 has caused certain fundamental elements of the Directive to receive less than adequate attention. As discussed earlier, several agencies had mistakenly decided to not implement PDD 63 because they believed they were exempt from the Directive and have not established performance measures. Additionally, most agencies will not have benefited from Project Matrix by the time the program could cease to exist. Further, we found that the GSA's Federal Sector Liaison has provided limited direction or assistance to the agencies. Finally, the CIAO's Expert Review Team (ERT), which has reviewed and furnished comments to 22 agencies regarding their CIP plans, is no longer functioning.[8]

[8]The Department of Commerce fiscal year 2001 budget request states that the National Institute of Standards and Technology (NIST) will establish a permanent ERT to replace the interim ERT at the National CIAO. In December 2000, NIST authorized the establishment of a Computer Security Expert Assist Team to review agency security practices, policies, and procedures. As of March 12, 2001, NIST had not activated the Computer Security Expert Assist Team due to a Federal hiring freeze.

We suggest that the Director, Office of Management and Budget, assign one organization the appropriate leadership responsibility and authority for overseeing the implementation of PDD 63 and for achieving government-wide, full operational capability by May 2003.

Advancing Beyond the Planning Phase

Some agencies have not performed vulnerability assessments of their critical infrastructure assets or prepared the related remediation plans. This condition occurred because the budget requests that the agencies submitted to the OMB were not sufficiently detailed for OMB to consider in funding the agencies' CIP requirements. The agencies' ability to prepare detailed requests, however, requires that the agencies perform vulnerability assessments and develop remediation plans, an undertaking for which the agencies have lacked funding or have been unwilling to fund from other parts of their approved budgets. Accordingly, some agencies have not advanced their CIP programs beyond the planning phase almost 3 years after President Clinton signed PDD 63.

The National Plan for Information Systems Protection, Version 1.0, "An Invitation to a Dialogue,"[9] states that the quality of the agencies' CIP budget requests did not meet OMB's expectations for the following reasons.

> Agency budget systems don't readily support collection of CIP data. Until these systems are modified, collection of information on CIP programs and budgets will be manual and inexact. The newness of CIP also means that the government is still on the steep part of a precipitous learning curve. Individual Agencies are still grappling with the issue internally and the interagency process is still coming together. . . . When OMB issued its first CIP Budget Data Request (BDR) last year, it sought information at an activity level. But because of inadequate activity descriptions and data presentation problems, it was unable to consolidate the data, making it difficult to identify programmatic duplications and gaps that point up inconsistencies needing analysis and remedy. All this reduced confidence in the data.

On March 8, 2000, OMB informed agencies that "extremely detailed" information regarding needed corrective actions must accompany the budget data submitted to OMB. This request also appears in OMB's Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," dated February 28, 2000, to remind agencies of OMB criteria for incorporating and funding security as part of the agencies' information technology systems and architectures and of the decision criteria that OMB will use to evaluate security for information systems investments. OMB issued the memorandum pursuant to the Clinger-Cohen Act, which directs OMB to develop a mechanism to analyze, track, and evaluate the risks and results of an agency's major capital investments in information systems. OMB will incorporate the criteria into future revisions of OMB Circular A-130. Further, OMB requires agencies to apply the criteria in conjunction with Memorandum M-97-02, "Funding Information Systems Investments," which emphasizes the need for well-justified budget requests.

As previously stated, the President intends that the United States take all necessary measures to swiftly eliminate any significant vulnerability to its critical infrastructures. Accordingly, unless

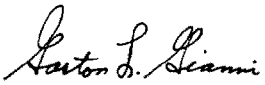
[9] The National Plan, issued by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, is the first attempt by a national Government to design a way to protect its cyberspace.

additional funding is forthcoming, some agencies may need to reprioritize application of existing funding to meet PDD 63 requirements. Our suggestion to establish performance measures should provide the additional attention needed to ensure that funding is made available to implement PDD 63.

* * * * *

We appreciate your consideration of the matters discussed in this letter. If you have any questions or comments, please call Russell A. Rau, NASA Assistant Inspector General for Auditing, at (202) 358-4458.

Sincerely,



Gaston L. Gianni, Jr.
PCIE Vice Chair

Barry R. Snyder
ECIE Vice Chair

Enclosure

Identical letter directed to:
Mr. Richard Clarke
National Coordinator for Security, Infrastructure
Protection and Counter-Terrorism

Enclosure

PARTICIPATING OFFICES OF INSPECTOR GENERAL

Agency for International Development

Department of Agriculture

Department of Commerce

Department of Education

Department of Energy

Department of Health and Human Services

Department of Housing and Urban Development

Department of the Interior

Department of Justice

Department of State

Department of the Treasury

Federal Deposit Insurance Corporation

Federal Emergency Management Agency

Federal Reserve Board

General Services Administration

National Aeronautics and Space Administration

Nuclear Regulatory Commission

Office of Personnel Management

Railroad Retirement Board

Small Business Administration

Treasury Inspector General for Tax Administration

Reported Answers to Review Guide Questions

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
3	**Agencies**																Y	N	NA	No Answer	Total	
4																						
5																						
6	**ID of Critical Assets**														**SEE NOTE 1**							**PDD 63 Requirements**
7	**B1a**	Y	N	N	Y	N	N	Y	N	N	N	N	Y	N	Y Y Y	N	5	10			15	**People identified in MEI**
8	B1b	Y	N	N	Y	N	N	Y	N	Y	N	N	Y	N	Y N Y	N	6	9			15	
9	B1c	Y	N	N	Y	N	N	Y	N	Y	N	N	Y	N	Y Y Y	N	6	9			15	
10	B1d	Y		N	Y	N	N	Y	N	N	N	N	Y	N	Y N Y	N	5	9		1	15	
11	B1e	Y	N	N	Y	N	N	Y	Y	Y	N	N	Y	N	Y Y Y	Y	8	7			15	
12	B2	Y	N	N	N	N	N	Y	N	Y	N	N	Y	NA	Y N Y	N	5	9	1		15	
13	B2A	N		N	Y	N	N	Y	N	NA	N	N	Y	NA	N N N	N	3	9	2	1	15	
14	B3a	Y	N	N	Y	N	N	Y	N	Y	N	N	Y	Y	Y N Y	N	7	8			15	
15	B3b	Y	Y	Y	Y	N	Y	Y	N	Y	Y	Y	Y	Y	Y Y Y	N	12	3			15	**Y2K work used to ID MEI**
16	B3c	Y	N	N	N	N	N	Y	N	N	N	N	N	Y	N N Y	N	3	12			15	**MEI ID cost, life cyle, impact**
17	B3d	Y	Y	Y	Y	Y	Y	Y	N	N	N	N	Y	Y	Y N Y	N	10	5			15	
18	B3e	Y	N	Y	Y	N	N		NA	NA	NA	N	Y	Y	Y NA Y	N	6	5	3	1	15	
19																						
20	**VUL ASSMT**																					
21	**C1**	N	N	Y	N	N	N	N	N	Y	N	N	N	N	N N N	N	2	13			15	**Performed Initial Vul Assmt**
22	C2	NA	N	NA		N	NA	NA	N	Y	N	N	Y	Y	N N N	N	3	7	4	1	15	
23	C3	NA	N	NA	N	N	NA	NA	N	Y	N	N	N	NA	NA N NA	N	1	8	6		15	
24	C4	NA	N	Y	N	N	N	NA	N	Y	N	N	N	N	N N N	N	2	11	2		15	
25	C5	NA	N	Y	N	N	N	N	N	Y	N	N	N	N	N N NA	N	2	12	1		15	
26	C6	NA	N	Y	N	N	NA	NA	N	Y	NA	NA	N/A	NA	NA NA NA	N	2	5	8		15	
27	C7	Y	N	N	Y	Y		Y	Y	Y	N	N	Y	Y	Y N Y	Y	10	4		1	15	**Has Vul Assmt been deleg to CIO/CIAO**
28	C8	N	N	N	N	N	N	NA	N	Y	N	N	N/A	N	N N Y	N	1	12	2		15	
29	C9	N	N	N	Y	N	N	NA	N	N	N	N	Y	N	N NA Y	N	2	12	1		15	
30	C10	NA	N	NA	Y	N	NA	NA	NA	N	N	N	Y	N	NA N N	N	2	8	5		15	
31	C11	NA	N	NA	Y	N	NA	NA	NA	Y	N	N	N	N	N N N	N	2	8	5		15	
32	C12	Y	N	NA	N	N	N	NA	NA	N	N	N	N	N	N N N	N	1	11	3		15	
33	C13	Y	N	NA	Y	Y	NA	NA	NA	Y	N	N	Y	NA	NA Y Y	N	6	4	5		15	
34	C14	NA	N	NA	Y	N	NA	NA	NA	Y	Y	N	N	Y	NA NA NA	N	4	5	6		15	
35	C15	Y	NA	N	Y	Y	N	NA	NO ANS	Y	N		Y	NA	NA NA NA	N/A	5	3	5	2	15	
36																						
37																						
38																						
39	**Agencies without CIPP**																					
40																						
41																						
42																						
43																						
44	**LEGEND**																					
45	**Y - YES**																					
46	**N - NO**																					
47	**NA- Not Applicable**																					

EXCERPTS
OF

PCIE/ECIE Review Guide
Phase I

For use in reviewing an agency's

Critical Infrastructure Assurance Program

December 15, 1999

Prepared by: Office of Inspector General
National Aeronautics and Space Administration

Review Guide -- Table of Contents

I.	Introduction	1
II.	Objectives, Scope, and Methodology	2
III.	Acronyms	3
IV.	Special Instructions	3
V.	Criteria	4
VI.	Recent Audits	5
VII.	Milestones for Phases I through IV	5
VIII.	Review Steps	6
	General Steps	6
	Specific Steps	6
	A. Critical Infrastructure Planning	6
	B. Identification of Critical Assets	9
	C. Vulnerability Assessments	10
Appendix 1	Phase (Tier) I and II Agencies	12
Appendix 2	Model Role for the Inspector General in Critical Infrastructure Assurance	13
Appendix 3	Schedule of Review Results	14

VIII. Review Steps (Note: Steps apply only to critical cyber-based infrastructures)

General Steps

Objectives. *Identify past and present issues related to the agency's critical infrastructure, and the criteria and management roles and responsibilities related to its critical infrastructure. (These steps are intended to help identify work previously performed by your agency and to avoid unnecessary duplication of review effort. File the results with your working papers.)*

1. Identify agency internal and external management reports related to critical infrastructure. If recommendations were made in these reports, determine the status of actions taken to implement the recommendations.

2. Familiarize yourself with the criteria and organizational structure that your agency uses to manage its critical infrastructure.
   a. Identify the organization(s) in the agency having responsibility for interpreting Federal critical infrastructure guidance and developing agency infrastructure policies, procedures, and standards.
   b. Determine whether the agency has formalized its critical infrastructure protection (CIP) standards, policies, and procedures.

Specific Steps.[1] After an agency has established its critical infrastructure protection plans and policy, it should identify critical assets relevant to PDD 63, identify and analyze critical asset infrastructure dependencies and interdependencies, and conduct appropriate vulnerability assessments.

A. Critical Infrastructure Planning

Objective: *Determine whether departments and agencies*[2] *have developed an effective plan for protecting their critical cyber-based infrastructures.* ***Note: Answer all questions that follow on the Schedule of Review Results (Appendix 3). All "no" answers require information on the cause, effect, resolution, cost, and recommendation, when applicable.***

1. Has the agency completed its critical infrastructure protection plan (CIPP)? If no, determine when your agency plans to complete the CIPP.

2. If the agency does not plan to complete a CIPP, is it because the agency was not included among the Phase I and Phase II agencies specifically subject to PDD 63? (A list of Phase I/II agencies is provided in Appendix 1.)

3. If the answer to question A.2. is yes, then identify some of your agency's cyber-based assets that may be subject to PDD 63. (The White Paper for PDD 63 defines critical infrastructures as those

---

[1] Sources of information used to compile the general review guidance included the *White Paper - - The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*; NASA's draft *Critical Infrastructure Protection Plan*, dated January 1999; and the draft National Plan for Information System Protection, dated Setpember16, 1999.

[2] To simplify, departments and agencies are hereafter referred to as agencies

physical and cyber-based systems essential to the minimum operations of the economy and government.) For the cyber-based assets so identified, does agency management agree that any of them should be subject to PDD 63? Note: For those OIG's that answered question A.3., please submit the schedule and summary of review results for work performed through this step. Your participation in this review is then finished.

4. For those agencies that have prepared a CIPP, did the Critical Infrastructure Coordination Group sponsor an "expert review process" for the CIPP, as required? (If yes, obtain a copy of the Expert Review Team (ERT) results for your agency. Refer to the applicable ERT results when performing the remaining steps in this Review Guide. If an ERT review was not performed, then determine the "cause" and continue with the remaining steps.

5. If the Critical Infrastructure Coordination Group has completed the expert review and found the CIPP deficient, has the agency taken adequate remedial action(s)?

6. Does the CIPP require the appointment of a Chief Infrastructure Assurance Officer (CIAO) who will have overall responsibility for protecting the agency's critical infrastructure?

7. Has the agency appointed a CIAO?

8. Does the CIPP require the agency to identify its cyber-based MEI?

9. Does the CIPP identify a milestone for identifying its cyber-based MEI?

10. Does the agency CIPP require an evaluation of new assets to determine whether they should be included in its MEI?

11. Does the CIPP require the agency to perform vulnerability assessments of its cyber-based MEI?

12. Does the CIPP require periodic updates of the assessments?

13. Does the CIPP identify milestones for completing the vulnerability assessments?

14. Does the CIPP require risk mitigation relative to potential damage stemming from each vulnerability?

15. Does the CIPP provide for periodic testing and re-evaluation of risk mitigation steps (policies, procedures, and controls) by agency management?

16. Does the CIPP provide a milestone for taking steps to mitigate risks?

17. Does the CIPP require establishment of an emergency management program?

18. If the answer to number 17 is yes, does the CIPP specify that the emergency management program include:

a. Incorporation of indications and warnings?
b. Incident collection, reporting, and analysis?
c. Response and continuity of operation plans?
d. A system for responding to significant infrastructure attacks, while the attacks are underway, with the goal of isolating and minimizing damage?
e. Notification to OIG criminal investigators of infrastructure attacks?

19. Does the CIPP require establishment of a system for quickly reconstituting minimum required capabilities following a successful infrastructure attack?

20. Does the CIPP identify a milestone for establishing the emergency management program?

21. Does the CIPP require a review of existing policies and procedures to determine whether the agency should revise them to reflect PDD 63 requirements?

22. Does the CIPP identify a milestone for reviewing existing policies and procedures?

23. Does the CIPP require the agency to ensure that security planning procedures are being incorporated into the basic design of new programs that include critical infrastructures, including provisions for:

a. Risk management and assessments?
b. Security plans for IT systems?
c. Security for command, control, and communications?
d. Identification of classified or sensitive information?
e. Awareness and training measures to be taken for each program?

24. Does the CIPP identify a milestone for establishing procedures to ensure that the agency incorporates security planning into the basic design of new programs?

25. Does the CIPP require the agency to incorporate its CIP functions into its strategic planning and performance measurement frameworks?

26. Does the CIPP identify a milestone for incorporating its critical infrastructure protection functions into its strategic planning and performance measurement frameworks?

27. Does the CIPP require agencies to identify resource and organizational requirements for implementing PDD 63?

28. Does the CIPP identify a milestone for identifying resource and organizational requirements for implementing PDD 63?

29. Does the CIPP require the agency to establish a program to ensure that it has the personnel and skills necessary to implement a sound infrastructure protection program?

30. Does the CIPP identify a milestone for establishing a program that would ensure the agency has the personnel and skills necessary to implement a sound infrastructure protection program?

31. Does the CIPP require the agency to establish effective CIP coordination with other applicable entities (foreign, state and local governments, and industry)?

32. Does the CIPP identify a milestone for establishing effective CIP coordination with other applicable entities (foreign, state and local governments, and industry)?

33. Do the agency's plans for the continuous/periodic review of its threat environment appear adequate, and is the agency complying with these plans?

B. Identification of Critical Assets

Objective. *Determine whether agencies have identified their cyber-based MEI and interdependencies.*[3]

1. Has the agency identified the following cyber-based MEI:
   a. People? (Staff, management - - including security management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission.)
   b. Technology? (All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.)
   c. Applications? (All application systems, internal and external, utilized in support of the core process.)
   d. Data? (All data - - electronic and hard copy - - and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or input into a computer, stored and processed there, or transmitted on some digital/communication's channel.)
   e. Facilities? (All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above in question B.1.)

2. Were the criteria used by the agency to identify its MEI consistent with the criteria used by the CIAO to identify agency MEI? (See footnote 1, page 1, for CIAO definition of agency MEI.)
   Added step: B2a. Did your agency use the CIAO infrastructure asset evaluation survey to identify its MEI assets?

3. Evaluate the adequacy of the agency's efforts to identify MEI and MEI interdependencies with applicable Federal agencies, state and local government activities, and industry.

---

[3] Interdependence is defined by the National Plan for Information Systems Protection as "Dependence among elements or sites of different infrastructures, and therefore, effects by one infrastructure upon another."

a. Has the agency identified assets consistent with the MEI as defined in question B.2?
b. Did the agency use the results of itsYear 2000 (Y2K) work in identifying the MEI?

c. Did the asset identification process include a determination of its estimated replacement costs, planned life cycle, and potential impact to the agency if the asset is rendered unusable?
d. Has the agency established milestones for identifying and reviewing their MEI?
e. Is the agency meeting its milestones?

*C. **Vulnerability Assessments***

***Objective**. Determine whether agencies have adequately (1) identified the threats, vulnerabilities and potential magnitude of harm to their cyber-based MEI that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of the their critical cyber-based infrastructure investments, and (2) developed remediation plans to address the risks identified.*

Background: A vulnerability assessment is a systematic examination of the ability of a system or application, including current security procedures and controls, to withstand assault. Agencies can use vulnerability assessments to identify weaknesses that could be exploited and to predict the effectiveness of additional security measures in protecting information resources from attack.

The vulnerability assessment reviews actions, devices, policies, procedures, techniques, and other factors that potentially place an agency's critical asset elements at risk. The outcome of the assessment is a list of flaws or omissions in controls (vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or availability of resources that are essential to critical assets.

Gathering reliable information to perform vulnerability assessments requires teams of security specialists to perform structured interviews and to review all the written documents available for each area of control and each critical asset element.

1. Has the agency performed and documented an initial vulnerability assessment and developed remediation plans for its MEI?

2. Did the vulnerability assessments address the threat type and magnitude of the threat, the source of the threats, existing protection measures, the probability of occurrence, damage that could result from a successful attack, and the likelihood of success if such an attack occurred?

3. Did the remediation plans address the vulnerabilities found during the assessment?

4. Has the agency determined the level of protection currently in place for its MEI?

5. Has the agency identified the actions that must be taken before it can achieve a reasonable level of protection for its MEI?

6. If your answer to number 5 is yes, then has the agency developed a related implementation plan and mechanism to monitor such implementation?

7. Has the agency delegated responsibility for vulnerability assessments to the agency CIO?

8. Has the agency adopted a multi-year funding plan that addresses the identified threats?

9. Has the agency reflected the cost of implementing a multi-year vulnerability remediation plan in its FY 2001 budget submission to OMB?

10. Did the vulnerability assessments query national threat guidance for international, domestic, and state-sponsored terrorism/information warfare (e.g., from the Department of Defense, FBI, NSA, and other Federal and State agencies)?

11. Has the agency prioritized the threats according to their relative importance?

12. Has the agency assessed the vulnerability of its MEI to failures that could result from interdependencies with applicable Federal agencies, state and local government activities, and private sector providers of telecommunications, electrical power, and other infrastructure services?

13. Do the processes used to identify and reflect new threats to the agency's MEI appear adequate?

14. Do the results of the vulnerability assessments necessitate revisions to agency policies that govern the management and protection of agency MEI?

15. Did the results of the ERT coincide with answers derived from questions A.1 through C.14?

January 16, 2001

M-01-08

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jack Lew
Director

SUBJECT: Guidance On Implementing the Government Information Security Reform Act

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform." It amends the Paperwork Reduction Act (PRA) of 1995 by enacting a new subchapter on "Information Security." The Act primarily addresses the program management and evaluation aspects of security. It covers unclassified and national security systems and creates the same management framework for each. At the policy level, the two types of systems remain separate. The Act became effective on November 29th and sunsets in two years.

The attachment provides guidance to agencies on carrying out the Act. The guidance focuses on unclassified Federal systems and addresses only those areas of the legislation that introduce new or modified requirements. The Act requires for both unclassified and national security programs: 1) annual agency program reviews; 2) annual Inspector General (IG) evaluations; 3) agency reporting to OMB the results of IG evaluations for unclassified systems and audits of IG evaluations for national security programs; and 4) an annual OMB report to Congress summarizing the materials received from agencies. Agencies will submit this information beginning in 2001 as part of the budget process.

The guidance also refers to some of the Act's provisions for national security systems. Unless otherwise specified, implementation of those provisions must be consistent with existing Presidential directives regarding national security systems.

This Act seeks to ensure proper management and security for the information resources supporting Federal operations and assets. It is particularly important as we move towards a more effective electronic government.

Please direct any questions about this guidance to Kamela White in the Office of Management and Budget at 202-395-3630, kgwhite@omb.eop.gov.

Attachment

Guidance On Implementing the Government Information Security Reform Act
Title X, subtitle G of the 2001 Defense Authorization Act (P.L. 106-398)

Part 1: **General Overview**

A. How does the Security Act affect existing security policy and authorities?
B. Does the Security Act pertain to existing agency systems?
C. Does the Security Act pertain to contractor systems?
D. How does the Security Act's new definition of "mission critical system" affect agency security responsibilities?
E. What is the relationship between the new Security Act and PDD-63, "Critical Infrastructure Protection?"
F. What are the relationships between the agency-wide security program and agency-wide security plan? Who is responsible for these and do individual systems still require security plans?

Part 2: **Agency Responsibilities**

A. What new agency responsibilities are found in the Security Act?
B. What are the responsibilities of the agency head?
C. What are the responsibilities of program officials?
D. What are the responsibilities of the agency Chief Information Officer?

Part 3: **Inspector General Responsibilities**

A. What are the responsibilities of the agency Inspector General?

Part 4: **OMB Responsibilities**

A. What are OMB's responsibilities under the Security Act?
B. Will OMB be revising its security policies?

Part 5: **Reporting Requirements**

A. What does the Security Act require agencies to report?
B. What does the Security Act require OMB to report?

Part 6: **Additional Responsibilities of Certain Agencies**

A. Department of Commerce
B. Department of Defense and the Intelligence Community
C. Department of Justice
D. General Services Administration
E. Office of Personnel Management

Part 1: General Overview

On October 30, 2000, the President signed into law the FY 2001 Defense Authorization Act (P.L. 106-398) including Title X, subtitle G, "Government Information Security Reform (The Security Act)." The Security Act was effective on November 29th and sunsets in two years.

The Security Act amends the Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. Chapter 35), by enacting a new subchapter on "Information Security" which primarily addresses the program management and evaluation aspects of security. This Act applies to all agencies covered by the PRA. It covers programs for both unclassified and national security systems and within the agencies creates the same management framework for each. At the policy level, the two programs remain separate. The Security Act requires annual agency program reviews, annual Inspector General security evaluations, agency reporting to OMB, and an annual OMB report to Congress.

The following guidance focuses on unclassified Federal systems and addresses only those areas of the legislation that introduce new or modified requirements or that otherwise benefit from clarification. In several locations, this guidance refers to some of the Security Act's provisions for national security systems. Unless otherwise specified, implementation of those provisions will be consistent with existing Presidential directives regarding national security information and systems.

A. How does the Security Act affect existing security policy and authorities?

For unclassified systems, OMB retains its existing policy authority under the PRA and the Clinger-Cohen Act of 1996.

Except for the new annual program reviews, the role of the agency Inspector General, and the annual reporting requirement, the Security Act essentially codifies the existing requirements of OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." The Security Act also requires agencies to incorporate security into the life cycle of agency information systems. For guidance on meeting this requirement, see OMB Memorandum 00-07, "Incorporating and Funding Security in Information Systems Investments," now incorporated into Section 8b(3) of OMB Circular A-130 (65 FR 77677; December 12, 2000). See, *www.cio.gov/docs/Recompiled_A-1301.htm.*

For national security systems, the Security Act directs OMB to delegate certain authorities to "the Secretary of Defense, the Director of Central Intelligence, and another agency head as designated by the President." The Security Act also directs OMB to delegate to the Secretary of Defense certain limited authorities concerning DOD unclassified mission critical systems. Delegations will be issued to appropriate agencies under separate cover, consistent with existing law and policy.

B. Does the Security Act pertain to existing agency systems?

Yes. The Security Act pertains to all systems supporting all operations and assets of an agency, including those systems currently in place or planned.

C. The Act states that DOD security policies also apply to DOD contractor systems. Do the security policies of other agencies also apply to their contractor's systems?

Yes. By using the Clinger-Cohen Act definition of information technology, the Security Act includes contractor systems. The Clinger-Cohen definition of information technology includes technology "used by the agency directly or is used by a contractor under contract to the agency. . ."

D. How does the Security Act's new definition of "mission critical system" affect agency security responsibilities?

The three-part definition for mission critical systems found in section 3532(b)(2) draws on the Computer Security Act of 1987 and the Clinger-Cohen Act. It is in the Security Act largely as a mechanism to keep separate the Security Act's requirements for policies concerning national security systems and unclassified systems. The Security Act reaffirms existing policy by requiring that agencies provide adequate security for all agency information, systems, operations, and assets.

The first part of the definition (section 3532(b)(2)(A)) references the Clinger-Cohen definition of national security systems. The second part (section 3532(b)(2)(B)) follows closely the Computer Security Act definition for systems processing national security information. The one change is that the word "secret" has been replaced by "classified" to reflect terminology used in Executive Order 12958, "Classified National Security Information." The Security Act combines these two types of systems for the purposes of establishing a policy framework that is separate and apart from the program for unclassified systems. Existing Presidential directives form the policy framework for securing national security systems. For the purposes of simplicity, this guidance refers to these systems as "national security systems."

The third part of the definition (section 3532(b)(2)(C)) is a modified Computer Security Act definition of systems processing sensitive, but unclassified, information.

By reiterating existing statutory definitions for national security systems and unclassified systems, the Security Act recognizes the distinctly different policy and oversight needs of the two programs and maintains the longstanding separation of the two.

E. What is the relationship between the new Security Act and PDD-63?, "Critical Infrastructure Protection?"

The Security Act compliments and does not conflict with PDD-63. Agencies should view their PDD-63 requirements in two ways. The first, especially for those agencies designated as lead agencies by the PDD, concerns interaction with industry: the new Security Act has no direct relationship to that role. The second concerns every agency's requirement to protect its critical infrastructures and, working with other agencies, to establish the Federal government as a model for security. These PDD requirements and the new Security Act (as is true for existing law and security policy) are complementary and not conflicting.

For agency operations and assets (including systems) the critical infrastructure protection program is largely an identification and prioritization effort. Within this effort an agency identifies its enterprise architecture, interdependencies, and relationships. Thereafter, it is incumbent upon the agency to apply applicable security policies (for unclassified systems or national security systems) to protect their operations and assets adequately while understanding the shared risk environment in which they operate. Again, within the agency asset context, the major thrust of critical infrastructure protection should be to concentrate on and ensure the security of those assets that are most critical. Agencies must ensure that they integrate their security programs and critical infrastructure protection efforts. For additional information on enterprise architecture see Section 8b of OMB Circular A-130 (65 FR 77677; December 12, 2000).

The agency plans, programs, and reports required by the Security Act (discussed elsewhere in this guidance) should reflect the integration of the two programs within the agency and include as appropriate agency critical infrastructure protection efforts.

A. What are the relationships between the agency-wide security program and agency-wide security plan? Who is responsible for these and do individual systems still require security plans?

Agency Chief Information Officers (CIO) should develop, implement, and maintain an agency-wide security program and describe the program in detail in the agency-wide plan. The Security Act reemphasizes the CIO's strategic, agency-wide security responsibility.

Each agency program official should develop, implement, and maintain a security program (and document it in a plan) that assesses risk and provides adequate security for the operations and assets of programs and systems under their control. Each system requires a plan. Where appropriate, individual plans may be consolidated into one plan that reflects a logical grouping or collection of systems, provided that the security controls for each system are fully documented. In consultation with the agency CIO, program officials should ensure that their individual program and plan are consistent with and incorporated into the agency-wide security program and plan.

Part 2: Agency Responsibilities

The Security Act names specific authorities, responsibilities, and functions for the agency, the head of the agency, agency program officials, and the CIO of the agency.

A. What new agency responsibilities are found in the Security Act?

Agency responsibilities set forth in the Security Act remain largely the same as those required by existing law and policy. The following are those that are most noteworthy.

1. Agency-wide Program Practiced Throughout Life Cycle

Each agency will develop and implement an agency-wide risk-based security program to provide information security throughout the life cycle of all systems supporting their operations and assets. This continues requirements of existing law and policy that direct agencies to ensure that risk-based security is an integral part of the enterprise architecture and is included in the capital planning and investment control process.

2. Incident Response Capability

As found in existing policy, all agency programs will include procedures for detecting, reporting, and responding to security incidents, including notifying and consulting with law enforcement officials, other offices and authorities, and the General Services Administration's Federal Computer Incident Response Capability (FedCIRC).

The intent of the incident handling provision is to ensure that each agency has both the technical and procedural means in place to detect and appropriately report security incidents and share information on common vulnerabilities. Policies and procedures should be documented and remove unnecessary internal obstacles to the timely reporting to the appropriate authorities within the agency (for example, security officials and Inspectors General) and with external organizations (for example, FedCIRC, law enforcement e.g., the National Infrastructure Protection Center, and national security). Agencies should refer to the CIO Council's October 2000 memorandum regarding interaction with FedCIRC (*www.cio.gov/docs/10_24FedCIRC_Note.htm*). The Security Act directs the Department of Justice to develop guidance on such reporting to law enforcement.

In light of the Security Act's new role for agency Inspectors General, they must be an integral part of the reporting process.

For national security systems, the Security Act establishes a companion requirement for reporting incidents concerning national security systems. Implementation will be consistent with existing national security policy directives and will preserve existing agency authorities and the need-to-know principles regarding classified national security information.

3. Annual Program Review

Agency program officials, in consultation with the CIO, must review each agency-wide information security program at least annually. This annual review should also include

reviews of all programs included in the agency-wide program. To promote consistent reviews across government, the CIO Council's Federal Information Technology Security Assessment Framework should form the basis for the annual program review. The National Institute of Standards and Technology will release in early 2001 a companion questionnaire to the Framework. See, *www.cio.gov/docs/federal_it_security_assessment_framework.htm.*

CIOs and program officials should coordinate their reviews with agency IGs to ensure consistent methodology and avoid unnecessary duplication of effort.

Agencies should report to OMB on their annual reviews when submitting their annual budget submissions, including an independent evaluation performed by the agency Inspector General.

4. Reporting Significant Deficiencies

Section 3534(c)(1)-(2) requires each agency to examine the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to: annual agency budgets; information resources management; performance and results based management under the Clinger-Cohen Act; program performance; and financial management.

The Security Act directs agencies to report findings of significant deficiencies in policy, procedures, or practice as a material weakness under the applicable criteria of other laws (see the Chief Financial Officers Act and the Federal Managers Financial Integrity Act). This provision does not establish new or expand existing criteria for determining material weaknesses within the requirements of those other laws. Rather, it establishes a logical relationship between agency security requirements and those other requirements. Thus, for example, the Federal Financial Management Improvement Act (FFMIA) and its implementing guidance does not recognize the concept of material weakness in computer security, as such, and therefore the findings from information security reviews would not necessarily need to be reported as separate findings under FFMIA (but would need to be taken into account in the analysis of financial systems performed under the Federal Managers' Financial Integrity Act.)

5. Annual Agency Performance Plan

Each agency, in consultation with the CIO, must include in their performance plan a description of the time periods for implementing the agency-wide security program that is required under section 3534(d)(1), and the budget, staffing, and training resources which are necessary to implement this security program.

B. What are the responsibilities of the agency head?

Each agency must ensure the integrity, confidentiality, authenticity, availability, and

nonrepudiation of information and information systems. Authenticity and nonrepudiation are security requirements addressed by the Government Paperwork Elimination Act and OMB Memorandum M-00-10, "OMB Procedures and Guidance on Implementing the Government Paperwork Elimination Act" (*www.cio.gov/docs/m00-10.html*).

Each agency must develop and implement information security policies, procedures, and control techniques sufficient to afford security protections commensurate with the risk and magnitude of harm. The head of each agency must also ensure that the agency practices its information security program throughout the life cycle of each agency system. For guidance on accomplishing this requirement, see OMB Circular A-130 Section 8b(3) (65 FR 77677; December 12, 2000) on incorporating and funding security in information systems investments.

The agency head must submit annually to the Director of OMB the results of an independent evaluation performed by the agency Inspector General and, for national security systems, an audit of the independent review. This evaluation must accompany the agency's annual budget submission and should include the results of all annual program reviews by program officials.

C. What are the responsibilities of program officials?

Program officials must assess the risks to the operations and assets over which they have control. This includes determining the appropriate levels of security and periodically testing and evaluating security controls and techniques to ensure that they are cost effective and that they enable, but do not unnecessarily impede, business operations.

Each information security program under the Security Act, with the exception of national security programs, is subject to the approval of the Director of OMB. In addition, agency program officials in consultation with the agency CIO, must review each program at least annually. To promote consistent reviews and reporting across government, the agency's CIO should work with program officials in performing these reviews using the CIO Council's Federal Information Technology Security Assessment Framework as a basis for these program reviews.

These provisions continue the principle in existing OMB policy that agency program officials, not security officers or CIOs, are ultimately responsible for the security of programs under their control. This includes determining the acceptable level of risk and adequate level of security. It is essential that program officials work closely with CIOs and other officials to ensure a complete understanding of risks, especially the increased risks resulting from interconnecting with other programs and systems over which the program officials have little or no control.

D. What are the responsibilities of the agency Chief Information Officer?

The CIO must administer the agency functions under the Security Act. Consistent with the PRA and the Clinger-Cohen Act, this reconfirms the role of the CIO in providing a strategic view of the agency's architecture and crosscutting security needs.

The CIO should designate a senior agency information security official who will report to the

CIO on the implementation and maintenance of the agency information security program and security policies. Most agencies have taken this action.

The CIO must participate in developing agency performance plans. These plans must include descriptions of the time periods required to implement the agency-wide security program required under section 3534(d)(1), and the budget, staffing, and training resources necessary to implement the program.

In fulfilling these requirements, agency CIOs must ensure that agency security programs integrate fully into the agency's enterprise architecture and capital planning and investment control processes. CIOs should work with agency program officials to ensure that the program officials understand and appropriately address risks, especially the increased risk resulting from interconnecting with other programs and systems over which the program officials have little or no control.

Part 3: Inspector General (IG) Responsibilities

A. What are the responsibilities of the agency IG?

IGs, or independent evaluators they choose, should perform an annual evaluation of the agency's security program and practices. This includes testing the effectiveness of security controls for "an appropriate subset of agency systems." Agencies without IGs should contract with an independent evaluator to perform the evaluation.

The appropriate subset provision reflects the realization that agencies cannot review all systems every year. Thus, IGs and other independent evaluators should identify and assess a logical representative sampling of systems that can be used to form the basis of a conclusion regarding the effectiveness of an agency's overall security program.

The IG or other independent evaluator may use any audit, evaluation, or report for the evaluation of agency programs or practices. This provision encourages IGs to use, to the extent practicable and weighing their quality, applicability and independence, those security program reviews, vulnerability assessments, audits, or evaluations performed by other experts. IGs should use results of the agency program reviews performed under the criteria of the CIO Council's Federal Information Technology Security Assessment Framework. Agency CIOs and program officials should work closely with agency IGs when developing their annual program review methodology. Furthermore, the annual program reviews and IG evaluations called for under this new legislation should be closely coordinated with IG audits and evaluations already being performed pursuant to the Chief Financial Officers Act under criteria from the General Accounting Office.

This approach will help ensure that agencies perform adequate, independent reviews of their security programs while preserving scarce resources and avoiding unnecessary duplication of effort. Moreover, this approach will help IGs and agency program officials avoid unnecessarily competing for expert personnel and other resources.

For the first report due in September 2001 with the agency budget submission, IGs should use the requirements and criteria found in GAO's FISCAM, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," current NIST guidance, the CIO Council Framework, and information gleaned during their review of any agency security incidents that may have occurred at the agency during the evaluation period. Clearly, IGs may also use any other sources that they deem appropriate. Prior to the second annual report, OMB will reevaluate the scope as appropriate.

IGs should use a cutoff date for their evaluation period that permits reporting the evaluation with the agency's annual budget submission. For national security systems, agencies must submit to OMB copies of audits of the annual evaluations, also due with the agency's budget submission. Consistent with current practice, IGs may also submit copies of audits or evaluations directly to OMB.

Part 4: OMB Responsibilities

The Security Act codifies existing OMB policy, OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources", and reiterates the requirements of the Computer Security Act of 1987, the PRA, and the Clinger-Cohen Act.

A. What are OMB's responsibilities under the Security Act?

Under the new Security Act, agency-wide security programs are subject to OMB "approval." OMB will implement this provision in a manner consistent with existing policy and practice. Generally, OMB approval will come from assessing performance through the agency self assessments, IG evaluations, and agency funding requests.

The Director of OMB has the authority to direct agencies to identify, use, and share best security practices; develop an agency-wide information security plan; incorporate information security principles and practices throughout the life cycles of the agency's information systems; and ensure that the agency's information security plan is practiced throughout the life cycles of the agency's information systems. Agencies should participate in the CIO Council's best security practices project to fulfill the first requirement.
The Director of OMB must submit to Congress an annual report that summarizes the program reviews and IG evaluations received from agencies.

In addition, the Director will establish government-wide policies for the management of programs that support cost-effective security of Federal information systems by promoting security as an integral component of each agency's business operations and include information technology architectures as defined under the Clinger-Cohen Act. Please see OMB Circular A-130 Section 8b(3) regarding incorporating and funding security in information systems investments.

B. Will OMB be revising its security policies?

Yes. Next spring OMB will begin revisions of OMB Circular A-130, Appendix III including conforming changes where necessary.

Part 5: Reporting Requirements

A. What does the Security Act require agencies to report?

The Security Act requires the agency head to report to OMB annually the results of each independent evaluation of the agency-wide information security program and practices of the agency. For national security systems, agencies are to provide the results of an audit of the evaluation.

Additionally, OMB will ask agencies to include the results of their annual program reviews also required by the Security Act and incorporate as appropriate reporting on their critical infrastructure protection efforts.

OMB will work with the agencies to develop a suitable form and format for agency reporting to OMB. Detailed guidance will be issued once a format is developed. It will ask agencies to submit their materials with their budget submissions.

B. What does the Security Act require OMB to report?

The Director of OMB will submit to Congress each year a report that summarizes the material received from agencies, including the annual IG evaluations, IG audits of evaluations of national security systems, and the program official's program reviews.

Part 6: Responsibilities of Certain Agencies

The Security Act charges the Department of Commerce, the Department of Defense and Intelligence Community, the Department of Justice, the General Services Administration, and the Office of Personnel Management with additional responsibilities.

A. Department of Commerce

The Department of Commerce (National Institute of Standards and Technology - NIST) retains its authorities and responsibilities as found in existing law and policy.

B. Department of Defense and the Intelligence Community

The Security Act directs the Secretary of Defense, the Director of Central Intelligence, and another agency head designated by the President to develop policies and guidelines for national security systems that are more stringent than those required for unclassified systems. This includes systems that are operated by the Department of Defense (DOD), a contractor of DOD, or another entity on behalf of DOD. The implementation of this provision will be consistent

with existing Presidential directives concerning the protection of national security information and systems.

1. Under what circumstances can agencies apply the more stringent national security controls to unclassified systems?

The Security Act provides that more stringent policies and procedures may be adopted by OMB or other agencies to the extent that such policies are consistent with OMB policies and procedures. As with existing policy, agencies may employ more stringent controls when they have identified a compelling need to do so and can articulate that need.

The Security Act reinforces existing law and OMB policy that directs agencies to provide whatever levels of cost-effective, risk-based security that they deem necessary to mitigate the risks to their operations and assets. If an agency determines that national security policies and procedures are necessary for protecting an unclassified system, they may use them, provided that it articulates the basis for this decision. Agencies will not receive funding for the system unless they provide adequate justification. See OMB Circular A-130 Section 8b(3) regarding incorporating and funding security in information systems investments for additional guidance.

The Security Act does not provide authority to the Secretary of Defense or the Intelligence Community to establish or promote policies for unclassified systems not under their control.

C. Department of Justice

The Attorney General will review and update guidance to agencies on legal remedies regarding security incidents, on ways to report to and work with law enforcement agencies, and on lawful uses of security techniques and technologies.
This guidance should establish agreed upon thresholds for agency reporting of security incidents to law enforcement authorities and provide to the agencies acceptable uses of security controls such as intrusion detection and keystroke monitoring that maximize security while appropriately preserving the privacy of individuals. This guidance will reflect consultation with OMB and the agencies and will be consistent with OMB policies concerning security and privacy.

D. General Services Administration

The Security Act conveys authorities and responsibilities to the General Services Administration (GSA) that are today found in OMB policy and reflect the transfer of FedCIRC operations from NIST to GSA. These authorities include updating guidance on addressing security considerations when acquiring information technology, assisting agencies in fulfilling their incident handling requirements, and assisting agencies in the acquisition of cost-effective security products, services, and incident response capabilities. All such guidance must be

consistent with and avoid unnecessary duplication of policy and guidance issued by OMB and NIST.

Beyond the authority to provide limited guidance described above, the Security Act does not provide any policy or guidance setting authority to GSA. From time-to-time, however, provided it is consistent with OMB policy and NIST guidance, GSA may issue operational procedures to assist agencies in improving the effectiveness of their incident handling capabilities. As has been the case with past practices, GSA will periodically report to OMB and NIST on findings, trends, and recommended remedies to causes of security incidents and vulnerabilities. OMB and NIST will use this information to inform the development of policy and guidance.

E. Office of Personnel Management

The Security Act conveys authorities and responsibilities to the Office of Personnel Management (OPM) that are today found in OMB policy. Additionally, it directs OPM to work with the National Science Foundation and other agencies on personnel and training initiatives for information security. Provided that adequate funds are appropriated, this language authorizes the establishment of a "Scholarship for Service" initiative and other Federal Cyber Services programs included in the President's FY 2001 budget.

Office of Management and Budget

CIRCULAR NO. A-130, Revised, (Transmittal Memorandum No. 4)

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Management of Federal Information Resources

1. Purpose
2. Rescissions
3. Authorities
4. Applicability and Scope
5. Background
6. Definitions
7. Basic Considerations and Assumptions
8. Policy
9. Assignment of Responsibilities
10. Oversight
11. Effectiveness
12. Inquiries
13. Sunset Review Date

Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals

Appendix II, Implementation of the Government Paperwork Elimination Act
Appendix III, Security of Federal Automated Information Resources
Appendix IV, Analysis of Key Sections

1. Purpose: This Circular establishes policy for the management of Federal information resources. OMB includes procedural and analytic guidelines for implementing specific aspects of these policies as appendices.

2. Rescissions: This Circular rescinds OMB Memoranda M-96-20, "Implementation of the Information Technology Management Reform Act of 1996;" M-97-02, "Funding Information Systems Investments;" M-97-09, "Interagency Support for Information Technology;" M-97-15, "Local Telecommunications Services Policy;" M-97-16, "Information Technology Architectures".

3. Authorities: OMB issues this Circular pursuant to the Paperwork Reduction Act (PRA) of 1980, as amended by the Paperwork Reduction Act of 1995 (44 U.S.C. Chapter 35); the Clinger-Cohen Act (also known as "Information Technology Management Reform Act of 1996") (Pub. L. 104-106, Division E); the Privacy Act, as amended (5 U.S.C. 552a); the Chief Financial Officers Act (31 U.S.C. 3512 et seq.); the Federal Property and Administrative Services Act, as amended (40 U.S.C. 487); the Computer Security Act of 1987 (Pub. L. 100-235); the Budget and Accounting Act, as amended (31 U.S.C. Chapter 11); the Government Performance and Results Act of 1993(GPRA); the Office of Federal Procurement Policy Act (41 U.S.C. Chapter 7); the Government Paperwork Elimination Act of 1998 (Pub. L. 105-277, Title XVII), Executive Order No. 12046 of March 27, 1978; Executive Order No. 12472 of April 3, 1984; and Executive Order No. 13011 of July 17, 1996.

4. Applicability and Scope:

a. The policies in this Circular apply to the information activities of all agencies of the executive branch of the Federal government.

b. Information classified for national security purposes should also be handled in accordance with the appropriate national security directives. National security emergency preparedness activities should be conducted in accordance with Executive Order No. 12472.

5. Background: The Clinger-Cohen Act supplements the information resources management policies contained in the PRA by establishing a comprehensive approach for executive agencies to improve the acquisition and management of their information resources, by:

1. focusing information resource planning to support their strategic missions;
2. implementing a capital planning and investment control process that links to budget formulation and execution; and
3. rethinking and restructuring the way they do their work before investing in information systems.

The PRA establishes a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner. To assist agencies in an integrated approach to information resources management, the PRA requires that the Director of OMB develop and implement uniform and consistent information resources management policies; oversee the development and promote the use of information management principles, standards, and guidelines; evaluate agency information resources management practices in order to determine their adequacy and efficiency; and determine compliance of such practices with the policies, principles, standards, and guidelines promulgated by the Director.

6. Definitions:

a. The term "agency" means any executive department, military department, government corporation, government controlled corporation, or other establishment in the executive branch of the Federal government, or any independent regulatory agency. Within the Executive Office of the President, the term includes only OMB and the Office of Administration.

b. The term "audiovisual production" means a unified presentation, developed according to a plan or script, containing visual imagery, sound or both, and used to convey information.

c. The term "capital planning and investment control process " means a management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

d. The term "Chief Information Officers Council" (CIO Council) means the Council established in Section 3 of Executive Order 13011.

e. The term "dissemination" means the government initiated distribution of information to the public. Not considered dissemination within the meaning of this Circular is distribution limited to government employees or agency contractors or grantees, intra- or inter-agency use or sharing of government information, and responses to requests for agency records under the Freedom of Information Act (5 U.S.C. 552) or Privacy Act.

f. The term "executive agency" has the meaning defined in section 4(1) of the Office of

Federal Procurement Policy Act (41 U.S.C. 403(1)).

g. The term "full costs," when applied to the expenses incurred in the operation of an information processing service organization (IPSO), is comprised of all direct, indirect, general, and administrative costs incurred in the operation of an IPSO. These costs include, but are not limited to, personnel, equipment, software, supplies, contracted services from private sector providers, space occupancy, intra-agency services from within the agency, inter-agency services from other Federal agencies, other services that are provided by State and local governments, and Judicial and Legislative branch organizations.

h. The term "government information" means information created, collected, processed, disseminated, or disposed of by or for the Federal Government.

i. The term "government publication" means information which is published as an individual document at government expense, or as required by law. (44 U.S.C. 1901)

j. The term "information" means any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual forms.

k. The term "information dissemination product" means any book, paper, map, machine-readable material, audiovisual production, or other documentary material, regardless of physical form or characteristic, disseminated by an agency to the public.

l. The term "information life cycle" means the stages through which information passes, typically characterized as creation or collection, processing, dissemination, use, storage, and disposition.

m. The term "information management" means the planning, budgeting, manipulating, and controlling of information throughout its life cycle.

n. The term "information resources" includes both government information and information technology.

o. The term "information processing services organization" (IPSO) means a discrete set of personnel, information technology, and support equipment with the primary function of providing services to more than one agency on a reimbursable basis.

p. The term "information resources management" means the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

q. The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

r. The term "information system life cycle" means the phases through which an information system passes, typically characterized as initiation, development, operation, and termination.

s. The term "information technology" means any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the

executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

t. The term "Information Technology Resources Board" (Resources Board) means the board established by Section 5 of Executive Order 13011.

u. The term "major information system" means an information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

v. The term "national security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which (1) involves intelligence activities; (2) involves cryptologic activities related to national security; (3) involves command and control of military forces; (4) involves equipment that is an integral part of a weapon or weapons system; or (5) is critical to the direct fulfillment of military or intelligence missions, but excluding any system that is to be administrative and business applications (including payroll, finance, logistics, and personnel management applications). The policies and procedures established in this Circular will apply to national security systems in a manner consistent with the applicability and related limitations regarding such systems set out in Section 5141 of the Clinger-Cohen Act (Pub. L. 104-106, 40 U.S.C. 1451). Applicability of Clinger-Cohen Act to national security systems shall include budget document preparation requirements set forth in OMB Circular A-11. The resultant budget document may be classified in accordance with the provisions of Executive Order 12958.

w. The term "records" means all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successoras evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the government or because of the informational value of the data in them. Library and museum material made or acquired and preserved solely for reference or exhibition purposes, extra copies of documents preserved only for convenience of reference, and stocks of publications and of processed documents are not included. (44 U.S.C. 3301)

x. The term "records management" means the planning, controlling, directing, organizing, training, promoting, and other managerial activities involved with respect to records creation, records maintenance and use, and records disposition in order to achieve adequate and proper documentation of the policies and transactions of the Federal Government and effective and economical management of agency operations. (44 U.S.C. 2901(2))

y. The term "service recipient" means an agency organizational unit, programmatic entity, or chargeable account that receives information processing services from an information processing service organization (IPSO). A service recipient may be either internal or external to the organization responsible for providing information resources services, but normally does not report either to the manager or director of the IPSO or to the same immediate supervisor.

7. Basic Considerations and Assumptions:

a. The Federal Government is the largest single producer, collector, consumer, and disseminator of information in the United States. Because of the extent of the government's information activities, and the dependence of those activities upon public cooperation, the management of Federal information resources is an issue of continuing importance to all Federal agencies, State and local governments, and the public.

b. Government information is a valuable national resource. It provides the public with knowledge of the government, society, and economy -- past, present, and future. It is a means to ensure the accountability of government, to manage the government's operations, to maintain the healthy performance of the economy, and is itself a commodity in the marketplace.

c. The free flow of information between the government and the public is essential to a democratic society. It is also essential that the government minimize the Federal paperwork burden on the public, minimize the cost of its information activities, and maximize the usefulness of government information.

d. In order to minimize the cost and maximize the usefulness of government information, the expected public and private benefits derived from government information should exceed the public and private costs of the information, recognizing that the benefits to be derived from government information may not always be quantifiable.

e. The nation can benefit from government information disseminated both by Federal agencies and by diverse nonfederal parties, including State and local government agencies, educational and other not-for-profit institutions, and for-profit organizations.

f. Because the public disclosure of government information is essential to the operation of a democracy, the management of Federal information resources should protect the public's right of access to government information.

g. The individual's right to privacy must be protected in Federal Government information activities involving personal information.

h. Systematic attention to the management of government records is an essential component of sound public resources management which ensures public accountability. Together with records preservation, it protects the government's historical record and guards the legal and financial rights of the government and the public.

i. Strategic planning improves the operation of government programs. The agency strategic plan will shape the redesign of work processes and guide the development and maintenance of an Enterprise Architecture and a capital planning and investment control process. This management approach promotes the appropriate application of Federal information resources.

j. Because State and local governments are important producers of government information for many areas such as health, social welfare, labor, transportation, and education, the Federal Government must cooperate with these governments in the management of information resources.

k. The open and efficient exchange of scientific and technical government information, subject to applicable national security controls and the proprietary rights of others, fosters excellence in scientific research and effective use of Federal research and development funds.

l. Information technology is not an end in itself. It is one set of resources that can improve the effectiveness and efficiency of Federal program delivery.

m. Federal Government information resources management policies and activities can affect, and be affected by, the information policies and activities of other nations.

n. Users of Federal information resources must have skills, knowledge, and training to manage information resources, enabling the Federal government to effectively serve the public through automated means.

o. The application of up-to-date information technology presents opportunities to promote fundamental changes in agency structures, work processes, and ways of interacting with the public that improve the effectiveness and efficiency of Federal agencies.

p. The availability of government information in diverse media, including electronic formats, permits agencies and the public greater flexibility in using the information.

q. Federal managers with program delivery responsibilities should recognize the importance of information resources management to mission performance.

r. The Chief Information Officers Council and the Information Technology Resources Board will help in the development and operation of interagency and interoperable shared information resources to support the performance of government missions.

8. Policy:

a. Information Management Policy

1. How will agencies conduct Information Management Planning?

Agencies must plan in an integrated manner for managing information throughout its life cycle. Agencies will:

(a) Consider, at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information dissemination;

(b) Consider the effects of their actions on members of the public and ensure consultation with the public as appropriate;

(c) Consider the effects of their actions on State and local governments and ensure consultation with those governments as appropriate;

(d) Seek to satisfy new information needs through interagency or intergovernmental sharing of information, or through commercial sources, where appropriate, before creating or collecting new information;

(e) Integrate planning for information systems with plans for resource allocation and use, including budgeting, acquisition, and use of information technology;

(f) Train personnel in skills appropriate to management of information;

(g) Protect government information commensurate with the risk and magnitude of harm that could result from the loss, misuse, or unauthorized access to or modification of such information;

(h) Use voluntary standards and Federal Information Processing Standards where appropriate or required;

(i) Consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented;

(j) Record, preserve, and make accessible sufficient information to ensure the management and accountability of agency programs, and to protect the legal and financial rights of the Federal Government;

(k) Incorporate records management and archival functions into the design, development, and implementation of information systems;

1. Provide for public access to records where required or appropriate.

2. What are the guidelines for Information Collection?

Agencies must collect or create only that information necessary for the proper performance of agency functions and which has practical utility.

3. What are the guidelines for Electronic Information Collection?

Executive agencies under Sections 1703 and 1705 of the Government Paperwork Elimination Act (GPEA), P. L. 105-277, Title XVII, are required to provide, by October 21, 2003, the (1) option of the electronic maintenance, submission, or disclosure of information, when practicable as a substitute for paper; and (2) use and acceptance of electronic signatures, when practicable. Agencies will follow the provisions in OMB Memorandum M-00-10, "Procedures and Guidance on Implementing of the Government Paperwork Elimination Act."

4. How must agencies implement Records Management?

Agencies will:

(a) Ensure that records management programs provide adequate and proper documentation of agency activities;

(b) Ensure the ability to access records regardless of form or medium;

(c) In a timely fashion, establish, and obtain the approval of the Archivist of the United States for retention schedules for Federal records; and

(d) Provide training and guidance as appropriate to all agency officials and employees and contractors regarding their Federal records management responsibilities.

5. How must an agency provide information to the public?

Agencies have a responsibility to provide information to the public consistent with their missions. Agencies will discharge this responsibility by:

(a) Providing information, as required by law, describing agency organization, activities, programs, meetings, systems of records, and other information holdings, and how the public may gain access to agency information resources;

(b) Providing access to agency records under provisions of the Freedom of Information Act and the Privacy Act, subject to the protections and limitations

provided for in these Acts;

(c) Providing such other information as is necessary or appropriate for the proper performance of agency functions; and

(d) In determining whether and how to disseminate information to the public, agencies will:

(i) Disseminate information in a manner that achieves the best balance between the goals of maximizing the usefulness of the information and minimizing the cost to the government and the public;

(ii) Disseminate information dissemination products on equitable and timely terms;

(iii) Take advantage of all dissemination channels, Federal and nonfederal, including State and local governments, libraries and private sector entities, in discharging agency information dissemination responsibilities;

(iv) Help the public locate government information maintained by or for the agency.

6. What is an Information Dissemination Management System?

Agencies will maintain and implement a management system for all information dissemination products which must, at a minimum:

(a) Assure that information dissemination products are necessary for proper performance of agency functions (44 U.S.C. 1108);

(b) Consider whether an information dissemination product available from other Federal or nonfederal sources is equivalent to an agency information dissemination product and reasonably fulfills the dissemination responsibilities of the agency;

(c) Establish and maintain inventories of all agency information dissemination products;

(d) Develop such other aids to locating agency information dissemination products including catalogs and directories, as may reasonably achieve agency information dissemination objectives;

(e) Identify in information dissemination products the source of the information, if from another agency;

(f) Ensure that members of the public with disabilities whom the agency has a responsibility to inform have a reasonable ability to access the information dissemination products;

(g) Ensure that government publications are made available to depository libraries through the facilities of the Government Printing Office, as required by law (44 U.S.C. Part 19);

(h) Provide electronic information dissemination products to the Government Printing Office for distribution to depository libraries;

(i) Establish and maintain communications with members of the public and with State and local governments so that the agency creates information dissemination

products that meet their respective needs;

(j) Provide adequate notice when initiating, substantially modifying, or terminating significant information dissemination products; and

(k) Ensure that, to the extent existing information dissemination policies or practices are inconsistent with the requirements of this Circular, a prompt and orderly transition to compliance with the requirements of this Circular is made.

7. How must agencies avoid improperly restrictive practices?

Agencies will:

(a) Avoid establishing, or permitting others to establish on their behalf, exclusive, restricted, or other distribution arrangements that interfere with the availability of information dissemination products on a timely and equitable basis; c) Set user charges for information dissemination products at a level sufficient to recover the cost of dissemination but no higher. They must exclude from calculation of the charges costs associated with original collection and processing of the information. Exceptions to this policy are:

(i) Where statutory requirements are at variance with the policy;

(ii) Where the agency collects, processes, and disseminates the information for the benefit of a specific identifiable group beyond the benefit to the general public;

(iii) Where the agency plans to establish user charges at less than cost of dissemination because of a determination that higher charges would constitute a significant barrier to properly performing theagency's functions, including reaching members of the public whom the agency has a responsibility to inform; or

(iv) Where the Director of OMB determines an exception is warranted.

8. How will agencies carry out electronic information dissemination?

Agencies will use electronic media and formats, including public networks, as appropriate and within budgetary constraints, in order to make government information more easily accessible and useful to the public. The use of electronic media and formats for information dissemination is appropriate under the following conditions:

(a) The agency develops and maintains the information electronically;

(b) Electronic media or formats are practical and cost effective ways to provide public access to a large, highly detailed volume of information;

(c) The agency disseminates the product frequently;

(d) The agency knows a substantial portion of users have ready access to the necessary information technology and training to use electronic information dissemination products;

(e) A change to electronic dissemination, as the sole means of disseminating the product, will not impose substantial acquisition or training costs on users, especially State and local governments and small business entities.

9. What safeguards must agencies follow?

Agencies will:

(a) Ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information;

(b) Limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions;

(c) Limit the sharing of information that identifies individuals or contains proprietary information to that which is legally authorized, and impose appropriate conditions on use where a continuing obligation to ensure the confidentiality of the information exists;

(d) Provide individuals, upon request, access to records about them maintained in Privacy Act systems of records, and permit them to amend such records as are in error consistent with the provisions of the Privacy Act.

b. How Will Agencies Manage Information Systems and Information Technology?

(1) How will agencies use capital planning and investment control process?

Agencies must establish and maintain a capital planning and investment control process that links mission needs, information, and information technology in an effective and efficient manner. The process will guide both strategic and operational IRM, IT planning, and the Enterprise Architecture by integrating the agency's IRM plans, strategic and performance plans prepared pursuant to the Government Performance and Results Act of 1993, financial management plans prepared pursuant to the Chief Financial Officer Act of 1990 (31 U.S.C. 902a5), acquisition under the Federal Acquisition Streamlining Act of 1994, and the agency's budget formulation and execution processes. The capitalplanning and investment control process includes all stages of capital programming, including planning, budgeting, procurement, management, and assessment.

As outlined below, the capital planning and investment control process has three components: selection, control, and evaluation. The process must be iterative, with inputs coming from all of the agency plans and the outputs feeding into the budget and investment control processes. The goal is to link resources to results (for further guidance on Capital Planning refer to OMB Circular A-11). The agency's capital planning and investment control process must build from the agency's current Enterprise Architecture (EA) and its transition from current architecture to target architecture. The Capital Planning and Investment Control processes must be documented, and provided to OMB consistent with the budget process. The Enterprise Architecture must be documented and provided to OMB as significant changes are incorporated.

(a) What plans are associated with the capital planning and investment control process?

In the capital planning and investment control process, there are two separate and distinct plans that address IRM and IT planning requirements for the agency. The IRM Strategic Plan is strategic in nature and addresses all information resources management of the agency. Agencies must develop and maintain the agency Information Resource Management Strategic Plan (IRM) as required by 44 U.S.C. 3506 (b) (2). IRM Strategic Plans should support the agency Strategic Plan

required in OMB Circular A-11, provide a description of how information resources management activities help accomplish agency missions, and ensure that IRM decisions are integrated with organizational planning, budget, procurement, financial management, human resources management, and program decisions.

The IT Capital Plan is operational in nature, supports the goals and missions identified in the IRM Strategic Plan, is a living document, and must be updated twice yearly. This IT Capital Plan is theimplementation plan for the budget year. The IT Capital Plan should also reflect the goals of the agency's Annual Performance Plan, the agency's Government Paperwork Elimination Act (GPEA) Plan, the agency's EA, and agency's business planning processes. The IT Capital Plan must be submitted annually to OMB with the agency budget submission. annually. The IT Capital Plan must include the following components:

(i) A component, derived from the agency's capital planning and investment control process under OMB Circular A-11, Section 300 and the OMB Capital Programming Guide, that specifically includes all IT Capital Asset Plans for major information systems or projects. This component must also demonstrate how the agency manages its other IT investments, as required by the Clinger-Cohen Act.

(ii) A component that addresses two other sections of OMB Circular A-11: a section for Information on Financial Management, including the Report on Financial Management Activities and the Agency's Financial Management Plan, and a section entitled Information Technology, including the Agency IT Investment Portfolio.

(iii) A component, derived from the agency's capital planning and investment control process, that demonstrates the criteria it will use to select the investments into the portfolio, how it will control and manage the investments, and how it will evaluate the investments based on planned performance versus actual accomplishments.

(iv) A component that includes a summary of the security plan from the agency's five-year plan as required by the PRA and Appendix III of this Circular. The plan must demonstrate that IT projects and the EA include security controls for components, applications, and systems that are consistent with the agency's Enterprise Architecture; include a plan to manage risk; protect privacy and confidentiality; and explain any planned or actual variance from National Institute of Standards and Technology(NIST) security guidance.

(b) What must an agency do as part of the selection component of the capital planning process?

It must:

(i) Evaluate each investment in information resources to determine whether the investment will support core mission functions that must be performed by the Federal government;

(ii) Ensure that decisions to improve existing information systems or develop new information systems are initiated only when no alternative private sector or governmental source can efficiently meet the need;

(iii) Support work processes that it has simplified or otherwise redesigned to reduce costs, improve effectiveness, and make maximum use of commercial,

off-the-shelf technology;

(iv) Reduce risk by avoiding or isolating custom designed components, using components that can be fully tested or prototyped prior to production, and ensuring involvement and support of users;

(v) Demonstrate a projected return on the investment that is clearly equal to or better than alternative uses of available public resources. The return may include improved mission performance in accordance with GPRA measures, reduced cost, increased quality, speed, or flexibility; as well as increased customer and employee satisfaction. The return should reflect such risk factors as the project's technical complexity, the agency's management capacity, the likelihood of cost overruns, and the consequences of under- or non-performance. Return on investment should, where appropriate, reflect actual returns observed through pilot projects and prototypes;

(vi) Prepare and update a benefit-cost analysis (BCA) for each information system throughout its life cycle. A BCA will provide a level of detail proportionate to the size of the investment, rely onsystematic measures of mission performance, and be consistent with the methodology described in OMB Circular No. A-94, "Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs";

(vii) Prepare and maintain a portfolio of major information systems that monitors investments and prevents redundancy of existing or shared IT capabilities. The portfolio will provide information demonstrating the impact of alternative IT investment strategies and funding levels, identify opportunities for sharing resources, and consider the agency's inventory of information resources;

(viii) Ensure consistency with Federal, agency, and bureau Enterprise architectures, demonstrating such consistency through compliance with agency business requirements and standards, as well as identification of milestones, as defined in the EA;

(ix) Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate IT capabilities within the same agency, from other agencies, or from the private sector;

(x) Ensure that the selected system or process maximizes the usefulness of information, minimizes the burden on the public, and preserves the appropriate integrity, usability, availability, and confidentiality of information throughout the life cycle of the information, as determined in accordance with the PRA and the Federal Records Act. This portion must specifically address the planning and budgeting for the information collection burden imposed on the public as defined by 5 CFR 1320;

(xi) Establish oversight mechanisms, consistent with Appendix III of this Circular, to evaluate systematically and ensure the continuing security, interoperability, and availability of systems and their data;

(xii) Ensure that Federal information system requirements do not unnecessarily restrict theprerogatives of state, local and tribal governments;

(xiii) Ensure that the selected system or process facilitates accessibility under the Rehabilitation Act of 1973, as amended.

(c) What must an agency do as part of the control component of the capital planning process?

It must:

(i) Institute performance measures and management processes that monitor actual performance compared to expected results. Agencies must use a performance based management system that provides timely information regarding the progress of an information technology investment. The system must also measure progress towards milestones in an independently verifiable basis, in terms of cost, capability of the investment to meet specified requirements, timeliness, and quality;

(ii) Establish oversight mechanisms that require periodic review of information systems to determine how mission requirements might have changed, and whether the information system continues to fulfill ongoing and anticipated mission requirements. These mechanisms must also require information regarding the future levels of performance, interoperability, and maintenance necessary to ensure the information system meets mission requirements cost effectively;

(iii) Ensure that major information systems proceed in a timely fashion towards agreed-upon milestones in an information system life cycle. Information systems must also continue to deliver intended benefits to the agency and customers, meet user requirements, and identify and offer security protections;

(iv) Prepare and update a strategy that identifies and mitigates risks associated with each information system;

(iv) Ensure that financial management systems conform to the requirements of OMB Circular No. A-127, "Financial Management Systems;"

(v) Provide for the appropriate management and disposition of records in accordance with the Federal Records Act.

(vi) Ensure that agency EA procedures are being followed. This includes ensuring that EA milestones are reached and documentation is updated as needed.

(d) What must an agency do as part of the evaluation component of the capital planning process?

It must:

(i) Conduct post-implementation reviews of information systems and information resource management processes to validate estimated benefits and costs, and document effective management practices for broader use;

(ii) Evaluate systems to ensure positive return on investment and decide whether continuation, modification, or termination of the systems is necessary to meet agency mission requirements.

(iii) Document lessons learned from the post-implementation reviews. Redesign oversight mechanisms and performance levels to incorporate acquired knowledge.

(iv) Re-assess an investment's business case, technical compliance, and compliance against the EA.

(v) Update the EA and IT capital planning processes as needed.

(2) The Enterprise Architecture

Agencies must document and submit their initial EA to OMB. Agencies must submit updates when significant changes to the Enterprise Architecture occur.

(a) What is the Enterprise Architecture?

An EA is the explicit description and documentation of the current and desired relationships among business and management processes and information technology. It describes the "current architecture" and "target architecture" to include the rules and standards and systems life cycle information to optimize and maintain the environment which the agency wishes to create and maintain by managing its IT portfolio. The EA must also provide a strategy that will enable the agency to support its current state and also act as the roadmap for transition to its target environment. These transition processes will include an agency's capital planning and investment control processes, agency EA planning processes, and agency systems life cycle methodologies. The EA will define principles and goals and set direction on such issues as the promotion of interoperability, open systems, public access, compliance with GPEA, end user satisfaction, and IT security. The agency must support the EA with a complete inventory of agency information resources, including personnel, equipment, and funds devoted to information resources management and information technology, at an appropriate level of detail. Agencies must implement the EA consistent with following principles:

(i) Develop information systems that facilitate interoperability, application portability, and scalability of electronic applications across networks of heterogeneous hardware, software, and telecommunications platforms;

(ii) Meet information technology needs through cost effective intra-agency and interagency sharing, before acquiring new information technology resources; and

(iii) Establish a level of security for all information systems that is commensurate to the risk and magnitude of the harm resulting from the loss, misuse, unauthorized access to, or modification of the information stored or flowing through these systems.

(b) How do agencies create and maintain the EA?

As part of the EA effort, agencies must use or create an Enterprise Architecture Framework. The Framework must document linkages between mission needs, information content, and information technology capabilities. The Framework must also guide both strategic and operational IRM planning.

Once a framework is established, an agency must create the EA. In the creation of an EA, agencies must identify and document:

(i) Business Processes - Agencies must identify the work performed to support its mission, vision and performance goals. Agencies must also document change agents, such as legislation or new technologies that will drive changes in the EA.

(ii) Information Flow and Relationships - Agencies must analyze the information utilized by the agency in its business processes, identifying the information used and the movement of the information. These information flows indicate where the information is needed and how the information is shared to support mission functions.

(iii) Applications - Agencies must identify, define, and organize the activities that capture, manipulate, and manage the business information to support business processes. The EA also describes the logical dependencies and relationships among business activities.

(iv) Data Descriptions and Relationships - Agencies must identify how data is created, maintained, accessed, and used. At a high level, agencies must define the data and describe the relationships among data elements used in the agency's information systems.

(v) Technology Infrastructure - Agencies must describe and identify the functional characteristics, capabilities, and interconnections of the hardware, software, and telecommunications.

(c) What are the Technical Reference Model and Standards Profile?

The EA must also include a Technical Reference Model (TRM) and Standards Profile.

(i) The TRM identifies and describes the information services (such as database, communications, intranet, etc.) used throughout the agency.

(ii) The Standards Profile defines the set of IT standards that support the services articulated in the TRM. Agencies are expected to adopt standards necessary to support the entire EA, which must be enforced consistently throughout the agency.

(iii) As part of the Standards Profile, agencies must create a Security Standards Profile that is specific to the security services specified in the EA and covers such services as identification, authentication, and non-repudiation; audit trail creation and analysis; access controls; cryptography management; virus protection; fraud prevention; detection and mitigation; and intrusion prevention and detection.

(3) How Will Agencies Ensure Security in Information Systems?

Agencies must incorporate security into the architecture of their information and systems to ensure that security supports agency business operations and that plans to fund and manage security are built into life-cycle budgets for information systems.

(a) To support more effective agency implementation of both agency computer security and critical infrastructure protection programs, agencies must implement the following:

(i) Prioritize key systems (including those that are most critical to agency operations);

(ii) Apply OMB policies and, for non-national security applications, NIST guidance to achieve adequate security commensurate with the level of risk and magnitude of harm;

(b) Agencies must make security's role explicit in information technology investments and capital programming. Investments in the development of new or the continued operation of existing informationsystems, both general support systems and major applications must:

(i) Demonstrate that the security controls for components, applications, and systems are consistent with, and an integral part of, the EA of the agency;

(ii) Demonstrate that the costs of security controls are understood and are explicitly incorporated into the life-cycle planning of the overall system in a manner consistent with OMB guidance for capital programming;

(iii) Incorporate a security plan that complies with Appendix III of this Circular and in a manner that is consistent with NIST guidance on security planning;

(iv) Demonstrate specific methods used to ensure that risks and the potential for loss are understood and continually assessed, that steps are taken to maintain risk at an acceptable level, and that procedures are in place to ensure that controls are implemented effectively and remain effective over time;

(v) Demonstrate specific methods used to ensure that the security controls are commensurate with the risk and magnitude of harm that may result from the loss, misuse, or unauthorized access to or modification of the system itself or the information it manages;

(vi) Identify additional security controls that are necessary to minimize risk to and potential loss from those systems that promote or permit public access, other externally accessible systems, and those systems that are interconnected with systems over which program officials have little or no control;

(vii) Deploy effective security controls and authentication tools consistent with the protection of privacy, such as public-key based digital signatures, for those systems that promote or permit public access;

(viii) Ensure that the handling of personal information is consistent with relevant government-wide and agency policies;

(ix) Describe each occasion the agency decides to employ standards and guidance that are more stringent than those promulgated by NIST to ensure the use of risk-based cost-effective security controls for non-national security applications;

(c) OMB will consider for new or continued funding only those system investments that satisfy these criteria. New information technology investments must demonstrate that existing agency systems also meet these criteria in order to qualify for funding.

(4) How Will Agencies Acquire Information Technology?

Agencies must:

(a) Make use of adequate competition, allocate risk between government and contractor, and maximize return on investment when acquiring information

technology;

(b) Structure major information systems into useful segments with a narrow scope and brief duration. This should reduce risk, promote flexibility and interoperability, increase accountability, and better match mission need with current technology and market conditions;

(c) Acquire off-the-shelf software from commercial sources, unless the cost effectiveness of developing custom software is clear and has been documented through pilot projects or prototypes; and

(d) Ensure accessibility of acquired information technology pursuant to the Rehabilitation Act of 1973, as amended (Pub. Law 105-220, 29 U.S.C.794d).

9. Assignment of Responsibilities:

a. All Federal Agencies. The head of each agency must:

1. Have primary responsibility for managing agency information resources;

2. Ensure that the agency implements appropriately all of the information policies, principles, standards, guidelines, rules, and regulations prescribed by OMB;

3. Appoint a Chief Information Officer, as required by 44 U.S.C. 3506(a), who must report directly to the agency head to carry out the responsibilities of the agencies listed in the Paperwork Reduction Act (44 U.S.C. 3506), the Clinger Cohen Act (40 U.S.C. 1425(b) & (c)), as well as Executive Order 13011. The head of the agency must consult with the Director of OMB prior to appointing a Chief Information Officer, and will advise the Director on matters regarding the authority, responsibilities, and organizational resources of the Chief Information Officer. For purposes of this paragraph, military departments and the Office of the Secretary of Defense may each appoint one official. The Chief Information Officer must, among other things:

   (a) Be an active participant during all agency strategic management activities, including the development, implementation, and maintenance of agency strategic and operational plans;

   (b) Advise the agency head on information resource implications of strategic planning decisions;

   (c) Advise the agency head on the design, development, and implementation of information resources.

      (i) Monitor and evaluate the performance of information resource investments through a capital planning and investment control process, and advise the agency head on whether to continue, modify, or terminate a program or project;

      (ii) Advise the agency head on budgetary implications of information resource decisions; and

   (d) Be an active participant throughout the annual agency budget process in establishing investment priorities for agency information resources;

4. Direct the Chief Information Officer to monitor agency compliance with the policies, procedures, and guidance in this Circular. Acting as an ombudsman, the Chief Information Officer must consider alleged instances of agency failure to comply with this Circular, and recommend or take appropriate corrective action. The Chief

Information Officer will report instances of alleged failure and their resolution annually to the Director of OMB, by February 1st of each year.

5. Develop internal agency information policies and procedures and oversee, evaluate, and otherwise periodically review agency information resources management activities for conformity with the policies set forth in this Circular;

6. Develop agency policies and procedures that provide for timely acquisition of required information technology;

7. Maintain the following, as required by the Paperwork Reduction Act (44 U.S.C. 3506(b)(4) and 3511) and the Freedom of Information Act (5 U.S.C. 552(g)): an inventory of the agency's major information systems, holdings, and dissemination products; an agency information locator service; a description of the agency's major information and record locator systems; an inventory of the agency's other information resources, such as personnel and funding (at the level of detail that the agency determines is most appropriate for its use in managing the agency's information resources); and a handbook for persons to obtain public information from the agency pursuant to these Acts.

8. Implement and enforce applicable records management policies and procedures, including requirements for archiving information maintained in electronic format, particularly in the planning, design and operation of information systems.

9. Identify to the Director of OMB any statutory, regulatory, and other impediments to efficient management of Federal information resources, and recommend to the Director legislation, policies, procedures, and other guidance to improve such management;

10. Assist OMB in the performance of its functions under the PRA, including making services, personnel, and facilities available to OMB for this purpose to the extent practicable;

11. Ensure that the agency:

    (a) cooperates with other agencies in the use of information technology to improve the productivity, effectiveness, and efficiency of Federal programs;

    (b) promotes a coordinated, interoperable, secure, and shared government wide infrastructure that is provided and supported by a diversity of private sector suppliers; and

    (c) develops a well-trained corps of information resource professionals.

12. Use the guidance provided in OMB Circular A-11, "Planning, Budgeting, and Acquisition of Fixed Assets," to promote effective and efficient capital planning within the organization;

13. Ensure that the agency provides budget data pertaining to information resources to OMB, consistent with the requirements of OMB Circular A-11,

14. Ensure, to the extent reasonable, that in the design of information systems with the purpose of disseminating information to the public, an index of information disseminated by the system will be included in the directory created by the Superintendent of Documents pursuant to 41 U.S.C. 4101.(Nothing in this paragraph authorizes the dissemination of information to the public unless otherwise authorized.)

15. Permit, to the extent practicable, the use of one agency's contract by another agency or

the award of multi-agency contracts, provided the action is within the scope of the contract and consistent with OMB guidance; and

16. As designated by the Director of OMB, act as executive agent for the government-wide acquisition of information technology.

b. Department of State. The Secretary of State must:

1. Advise the Director of OMB on the development of United States positions and policies on international information policy and technology issues affecting Federal government activities and the development of international information technology standards; and

2. Be responsible for liaison, consultation, and negotiation with foreign governments and intergovernmental organizations on all matters related to information resources management, including federal information technology. The Secretary must also ensure, in consultation with the Secretary of Commerce, that the United States is represented in the development of international standards and recommendations affecting information technology. These responsibilities may also require the Secretary to consult, as appropriate, with affected domestic agencies, organizations, and other members of the public.

c. Department of Commerce. The Secretary of Commerce must:

1. Develop and issue Federal Information Processing Standards and guidelines necessary to ensure the efficient and effective acquisition, management, security, and use of information technology, whiletaking into consideration the recommendations of the agencies and the CIO Council;

2. Advise the Director of OMB on the development of policies relating to the procurement and management of Federal telecommunications resources;

3. Provide OMB and the agencies with scientific and technical advisory services relating to the development and use of information technology;

4. Conduct studies and evaluations concerning telecommunications technology, and concerning the improvement, expansion, testing, operation, and use of Federal telecommunications systems, and advise the Director of OMB and appropriate agencies of the recommendations that result from such studies;

5. Develop, in consultation with the Secretary of State and the Director of OMB, plans, policies, and programs relating to international telecommunications issues affecting government information activities;

6. Identify needs for standardization of telecommunications and information processing technology, and develop standards, in consultation with the Secretary of Defense and the Administrator of General Services, to ensure efficient application of such technology;

7. Ensure that the Federal Government is represented in the development of national and, in consultation with the Secretary of State, international information technology standards, and advise the Director of OMB on such activities.

d. Department of Defense. The Secretary of Defense will develop, in consultation with the Administrator of General Services, uniform Federal telecommunications standards and guidelines to ensure national security, emergency preparedness, and continuity of government.

e. General Services Administration. The Administrator of General Services must:

1. Continue to manage the FTS2001 program and coordinate the follow-up to that program, on behalf of and with the advice of agencies;

2. Develop, maintain, and disseminate for the use of the Federal community (as requested by OMB or the agencies) recommended methods and strategies for the development and acquisition of information technology;

3. Conduct and manage outreach programs in cooperation with agency managers;

4. Be a liaison on information resources management (including Federal information technology) with State and local governments. GSA must also be a liaison with non-governmental international organizations, subject to prior consultation with the Secretary of State to ensure consistency with the overall United States foreign policy objectives;

5. Support the activities of the Secretary of State for liaison, consultation, and negotiation with intergovernmental organizations on information resource management matters;

6. Provide support and assistance to the CIO Council and the Information Technology Resources Board.

7. Manage the Information Technology Fund in accordance with the Federal Property and Administrative Services Act, as amended;

f. Office of Personnel Management. The Director, Office of Personnel Management, will:

1. Develop and conduct training programs for Federal personnel on information resources management, including end-user computing;

2. Evaluate periodically future personnel management and staffing requirements for Federal information resources management;

3. Establish personnel security policies and develop training programs for Federal personnel associated with the design, operation, or maintenance of information systems.

g. National Archives and Records Administration. The Archivist of the United States will:

1. Administer the Federal records management program in accordance with the National Archives and Records Act;

2. 2. Assist the Director of OMB in developing standards and guidelines relating to the records management program.

h. Office of Management and Budget. The Director of the Office of Management and Budget will:

1. Provide overall leadership and coordination of Federal information resources management within the executive branch;

2. Serve as the President's principal adviser on procurement and management of

Federal telecommunications systems, and develop and establish policies for procurement and management of such systems;

3. Issue policies, procedures, and guidelines to assist agencies in achieving integrated, effective, and efficient information resources management;

4. Initiate and review proposals for changes in legislation, regulations, and agency rocedures to improve Federal information resources management;

5. Review and approve or disapprove agency proposals for collection of information from the public, as defined by 5 CFR 1320.3;

6. Develop and maintain a Governmentwide strategic plan for information resources management.

7. Evaluate agencies' information resources management and identify cross-cutting information policy issues through the review of agency information programs, information collection budgets, information technology acquisition plans, fiscal budgets, and by other means;

8. Provide policy oversight for the Federal records management function conducted by the National Archives and Records Administration, coordinate records management policies and programs with other information activities, and review compliance by agencies with records management requirements;

9. Review agencies' policies, practices, and programs pertaining to the security, protection, sharing, and disclosure of information, in order to ensure compliance, with respect to privacy and security, with the Privacy Act, the Freedom of Information Act, the Computer Security Act, the GPEA, and related statutes;

10. Review proposed U.S. Government Position and Policy statements on international issues affecting Federal Government information activities, and advise the Secretary of State as to their consistency with Federal information resources management policy.

11. Coordinate the development and review by the Office of Information and Regulatory Affairs of policy associated with Federal procurement and acquisition of information technology with the Office of Federal Procurement Policy, and policies regarding management of financial management systems with the Office of Federal Financial Management.

12. Evaluate agency information resources management practices and programs and, as part of the budget process, oversee agency capital planning and investment control processes to analyze, track, and evaluate the risks and results of major capital investments in information systems;

13. Notify an agency if OMB believes that a major information system project requires outside assistance;

14. Provide guidance on the implementation of the Clinger-Cohen Act and on the management of information resources to the executive agencies, to the CIO Council, and to the Information Technology Resources Board; and

15. Designate one or more heads of executive agencies as executive agent for government-wide acquisitions of information technology.

10. Oversight:

a. The Director of OMB will use information technology planning reviews, fiscal budget reviews, information collection budget reviews, management reviews, and such other measures as the Director deems necessary to evaluate the adequacy and efficiency of each agency's information resources management and compliance with this Circular.

b. The Director of OMB may, consistent with statute and upon written request of an agency, grant a waiver from particular requirements of this Circular. Requests for waivers must detail the reasons why a particular waiver is sought, identify the duration of the waiver sought, and include a plan for the prompt and orderly transition to full compliance with the requirements of this Circular. Notice of each waiver request must be published promptly by the agency in the Federal Register, with a copy of the waiver request made available to the public on request.

11. Effectiveness: This Circular is effective upon issuance. Nothing in this Circular will be construed to confer a private right of action on any person.

12. Inquiries: All questions or inquiries should be addressed to the Office of Information and Regulatory Affairs, Office of Management and Budget, Washington, D.C. 20503. Telephone: (202) 395-3785.

13. Sunset Review Date: OMB will review this Circular three years from the date of issuance to ascertain its effectiveness.

Office of Management and Budget

Appendix III to OMB Circular No. A-130
Security of Federal Automated Information Resources

A. Requirements.

1. Purpose

This Appendix establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems established in accordance with OMB Circular No. A-123. The Appendix revises procedures formerly contained in Appendix III to OMB Circular No. A-130 (50 FR 52730; December 24, 1985), and incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

2. Definitions

The term:

a. "adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

b. "application" means the use of information resources (information and information technology) to satisfy a specific set of user requirements.

c. "general support system" or "system" means an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

d. "major application" means an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

3. Automated Information Security Programs. Agencies shall implement and maintain a

program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by the Office of Management and Budget, the Department of Commerce, the General Services Administration and the Office of Personnel Management (OPM). Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications:

a. Controls for general support systems.

1) Assign Responsibility for Security. Assign responsibility for security in each system to an individual knowledgeable in the information technology used in the system and in providing security for such technology.

2) System Security Plan. Plan for adequate security of each general support system as part of the organization's information resources management (IRM) planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 8(b) of this circular. Security plans shall include:

a) Rules of the System. Establish a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system. The rules shall be based on the needs of the various users of the system. The security required by the rules shall be only as stringent as necessary to provide adequate security for information in the system. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the system. They shall also include appropriate limits on interconnections to other systems and shall define service provision and restoration priorities. Finally, they shall be clear about the consequences of behavior not consistent with the rules.

b) Training. Ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system. Such training shall assure that employees are versed in the rules of the system, be consistent with guidance issued by NIST and OPM, and apprise them about available assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.

c) Personnel Controls. Screen individuals who are authorized to bypass significant technical and operational security controls of the system commensurate with the risk and magnitude of harm they could cause. Such screening shall occur prior to an individual being authorized to bypass controls and periodically thereafter.

d) Incident Response Capability. Ensure that there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations, consistent with NIST

coordination, and should assist the agency in pursuing appropriate legal action, consistent with Department of Justice guidance.

e) Continuity of Support. Establish and periodically test the capability to continue providing service within a system based upon the needs and priorities of the participants of the system.

f) Technical Security. Ensure that cost-effective security products and techniques are appropriately used within the system.

g) System Interconnection. Obtain written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems. Where connection is authorized, controls shall be established which are consistent with the rules of the system and in accordance with guidance from NIST.

3) Review of Security Controls. Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.

4) Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

b. Controls for Major Applications.

1) Assign Responsibility for Security. Assign responsibility for security of each major application to a management official knowledgeable in the nature of the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect it. This official shall assure that effective security products and techniques are appropriately used in the application and shall be contacted when a security incident occurs concerning the application.

2) Application Security Plan. Plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic IRM plan required by the Paperwork Reduction Act. Application security plans shall include:

a) Application Rules. Establish a set of rules concerning use of and behavior within the application. The rules shall be as stringent as necessary to provide adequate security for the application and the information in it. Such rules shall clearly delineate responsibilities and expected behavior of all individuals with access to the application. In addition, the rules shall be clear about the consequences of behavior not consistent with the rules.

b) Specialized Training. Before allowing individuals access to the application, ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application).

c) Personnel Security. Incorporate controls such as separation of duties, least privilege and individual accountability into the application and application rules as appropriate. In cases where such controls cannot adequately protect the application or information in it, screen individuals commensurate with the risk and magnitude of the harm they could cause. Such screening shall be done prior to the individuals' being authorized to access the application and periodically thereafter.

d) Contingency Planning. Establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

e) Technical Controls. Ensure that appropriate security controls are specified, designed into, tested, and accepted in the application in accordance with appropriate guidance issued by NIST.

f) Information Sharing. Ensure that information shared from the application is protected appropriately, comparable to the protection provided when information is within the application.

g) Public Access Controls. Where an agency's application promotes or permits public access, additional security controls shall be added to protect the integrity of the application and the confidence the public has in the application. Such controls shall include segregating information made directly accessible to the public from official agency records.

3) Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.

4) Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

4. Assignment of Responsibilities

a. Department of Commerce. The Secretary of Commerce shall:

1) Develop and issue appropriate standards and guidance for the security of sensitive information in Federal computer systems.

2) Review and update guidelines for training in computer security awareness and

accepted computer security practice, with assistance from OPM.

3) Provide agencies guidance for security planning to assist in their development of application and system security plans.

4) Provide guidance and assistance, as appropriate, to agencies concerning cost-effective controls when interconnecting with other systems.

5) Coordinate agency incident response activities to promote sharing of incident response information and related vulnerabilities.

6) Evaluate new information technologies to assess their security vulnerabilities, with technical assistance from the Department of Defense, and apprise Federal agencies of such vulnerabilities as soon as they are known.

b. Department of Defense. The Secretary of Defense shall:

1) Provide appropriate technical advice and assistance (including work products) to the Department of Commerce.

2) Assist the Department of Commerce in evaluating the vulnerabilities of emerging information technologies.

c. Department of Justice. The Attorney General shall:

1) Provide appropriate guidance to agencies on legal remedies regarding security incidents and ways to report and work with law enforcement concerning such incidents.

2) Pursue appropriate legal actions when security incidents occur.

d. General Services Administration. The Administrator of General Services shall:

1) Provide guidance to agencies on addressing security considerations when acquiring automated data processing equipment (as defined in section 111(a)(2) of the Federal Property and Administrative Services Act of 1949, as amended).

2) Facilitate the development of contract vehicles for agencies to use in the acquisition of cost-effective security products and services (e.g., back-up services).

3) Provide appropriate security services to meet the needs of Federal agencies to the extent that such services are cost-effective.

e. Office of Personnel Management. The Director of the Office of Personnel Management shall:

1) Assure that its regulations concerning computer security training for Federal civilian employees are effective.

2) Assist the Department of Commerce in updating and maintaining guidelines for training in computer security awareness and accepted computer security practice.

f. Security Policy Board. The Security Policy Board shall coordinate the activities of the Federal government regarding the security of information technology that processes classified information in accordance with applicable national security directives;

5. Correction of Deficiencies and Reports

a. Correction of Deficiencies. Agencies shall correct deficiencies which are identified through the reviews of security for systems and major applications described above.

b. Reports on Deficiencies. In accordance with OMB Circular No. A-123, "Management Accountability and Control", if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, it shall be included in the annual FMFIA report. Less significant deficiencies shall be reported and progress on corrective actions tracked at the appropriate agency level.

c. Summaries of Security Plans. Agencies shall include a summary of their system security plans and major application plans in the strategic plan required by the Paperwork Reduction Act (44 U.S.C. 3506).

B. Descriptive Information.

The following descriptive language is explanatory. It is included to assist in understanding the requirements of the Appendix.

The Appendix re-orients the Federal computer security program to better respond to a rapidly changing technological environment. It establishes government-wide responsibilities for Federal computer security and requires Federal agencies to adopt a minimum set of management controls. These management controls are directed at individual information technology users in order to reflect the distributed nature of today's technology.

For security to be most effective, the controls must be part of day-to-day operations. This is best accomplished by planning for security not as a separate activity, but as an integral part of overall planning.

"Adequate security" is defined as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

The Appendix no longer requires the preparation of formal risk analyses. In the past, substantial resources have been expended doing complex analyses of specific risks to systems, with limited tangible benefit in terms of improved security for the systems. Rather than continue to try to precisely measure risk, security efforts are better served by generally assessing risks and taking actions to manage them. While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used. This risk assessment approach should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. Additional guidance on effective risk assessment is available in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995).

Discussion of the Appendix's Major Provisions. The following discussion is provided to aid reviewers in understanding the changes in emphasis in the Appendix.

Automated Information Security Programs. Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. This Appendix emphasizes management controls affecting individual users of information technology. Technical and operational

controls support management controls. To be effective, all must interrelate. For example, authentication of individual users is an important management control, for which password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

Four controls are set forth: assigning responsibility for security, security planning, periodic review of security controls, and management authorization. The Appendix requires that these management controls be applied in two areas of management responsibility: one for general support systems and one for major applications.

The terms "general support system" and "major application" were used in OMB Bulletins Nos. 88-16 and 90-08. A general support system is "an interconnected set of information resources under the same direct management control which shares common functionality." Such a system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing enter including its operating system and utilities, a tactical radio network, or a shared information processing service organization. Normally, the purpose of a general support system is to provide processing or communications support.

A major application is a use of information and information technology to satisfy a specific set of user requirements that requires special management attention to security due to the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of the information in the application. All applications require some level of security, and adequate security for most of them should be provided by security of the general support systems in which they operate. However, certain applications, because of the nature of the information in them, require special management oversight and should be treated as major. Agencies are expected to exercise management judgement in determining which of their applications are major.

The focus of OMB Bulletins Nos. 88-16 and 90-08 was on identifying and securing both general support systems and applications which contained sensitive information. The Appendix requires the establishment of security controls in all general support systems, under the presumption that all contain some sensitive information, and focuses extra security controls on a limited number of particularly high-risk or major applications.

a. General Support Systems. The following controls are required in all general support systems:

1) Assign Responsibility for Security. For each system, an individual should be a focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. That responsibility should be assigned in writing to an individual trained in the technology used in the system and in providing security for such technology, including the management of security controls such as user identification and authentication.

2) Security Plan. The Computer Security Act requires that security plans be developed for all Federal computer systems that contain sensitive information. Given the expansion of distributed processing since passage of the Act, the presumption in the Appendix is that all general support systems contain some sensitive information which requires protection to assure its integrity, availability, or confidentiality, and therefore all systems require security plans.

Previous guidance on security planning was contained in OMB Bulletin No. 90-08. This-Appendix supersedes OMB Bulletin 90-08 and expands the coverage

of security plans from Bulletin 90-08 to include rules of individual behavior as well as technical security. Consistent with OMB Bulletin 90-08, the Appendix directs NIST to update and expand security planning guidance and issue it as a Federal Information Processing Standard (FIPS). In the interim, agencies should continue to use the Appendix of OMB Bulletin No. 90-08 as guidance for the technical portion of their security plans.

The Appendix continues the requirement that independent advice and comment on the security plan for each system be sought. The intent of this requirement is to improve the plans, foster communication between managers of different systems, and promote the sharing of security expertise.

This Appendix also continues the requirement from the Computer Security Act that summaries of security plans be included in agency strategic information resources management plans. OMB will provide additional guidance about the contents of those strategic plans, pursuant to the Paperwork Reduction Act of 1995.

The following specific security controls should be included in the security plan for a general support system:

a) Rules. An important new requirement for security plans is the establishment of a set of rules of behavior for individual users of each general support system. These rules should clearly delineate responsibilities of and expectations for all individuals with access to the system. They should be consistent with system-specific policy as described in "An Introduction to Computer Security: The NIST Handbook" (March 16, 1995). In addition, they should state the consequences of non-compliance. The rules should be in writing and will form the basis for security awareness and training.

The development of rules for a system must take into consideration the needs of all parties who use the system. Rules should be as stringent as necessary to provide adequate security. Therefore, the acceptable level of risk for the system must be established and should form the basis for determining the rules.

Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the assignment and limitation of system privileges, and individual accountability. Often rules should reflect technical security controls in the system. For example, rules regarding password use should be consistent with technical password features in the system. Rules may be enforced through administrative sanctions specifically related to the system (e.g. loss of system privileges) or through more general sanctions as are imposed for violating other rules of conduct. In addition, the rules should specifically address restoration of service as a concern of all users of the system.

b) Training. The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of all employees who are involved with the management, use or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency. Access provided to members of the public should be constrained by controls in the applications through which access is allowed, and training should be within the context of those controls. The

Appendix enforces such mandatory training by requiring its completion prior to granting access to the system. Each new user of a general support system in some sense introduces a risk to all other users. Therefore, each user should be versed in acceptable behavior -- the rules of the system -- before being allowed to use the system. Training should also inform the individual how to get help in the event of difficulty with using or security of the system.

Training should be tailored to what a user needs to know to use the system securely, given the nature of that use. Training may be presented in stages, for example as more access is granted. In some cases, the training should be in the form of classroom instruction. In other cases, interactive computer sessions or well-written and understandable brochures may be sufficient, depending on the risk and magnitude of harm.

Over time, attention to security tends to dissipate. In addition, changes to a system may necessitate a change in the rules or user procedures. Therefore, individuals should periodically have refresher training to assure that they continue to understand and abide by the applicable rules.

To assist agencies, the Appendix requires NIST, with assistance from the Office of Personnel Management (OPM), to update its existing guidance. It also proposes that OPM assure that its rules for computer security training for Federal civilian employees are effective.

c) Personnel Controls. It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

Individual accountability consists of holding someone responsible for his or her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. This may be done, for example, by looking for patterns of behavior by users.

Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

Nevertheless, in some instances, individuals may be given the ability to bypass some significant technical and operational controls in order to perform system administration and maintenance functions (e.g., LAN administrators or systems programmers). Screening such individuals in positions of trust will supplement technical, operational, and management controls, particularly where the risk and magnitude of harm is high.

d) Incident Response Capability. Security incidents, whether caused by viruses, hackers, or software bugs, are becoming more common. When faced

with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms. Awareness and training for individuals with access to the system should include how to use the system's incident response capability.

To be fully effective, incident handling must also include sharing information concerning common vulnerabilities and threats with those in other systems and other agencies. The Appendix directs agencies to effectuate such sharing, and tasks NIST to coordinate those agency activities government-wide.

The Appendix also directs the Department of Justice to provide appropriate guidance on pursuing legal remedies in the case of serious incidents.

e) Continuity of Support. Inevitably, there will be service interruptions. Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option. When automated support is not available, many functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service.

Decisions on the level of service needed at any particular time and on priorities in service restoration should be made in consultation with the users of the system and incorporated in the system rules. Experience has shown that recovery plans that are periodically tested are substantially more viable than those that are not. Moreover, untested plans may actually create a false sense of security.

f) Technical Security. Agencies should assure that each system appropriately uses effective security products and techniques, consistent with standards and guidance from NIST. Often such techniques will correspond with system rules of behavior, such as in the proper use of password protection.

The Appendix directs NIST to continue to issue computer security guidance to assist agencies in planning for and using technical security products and techniques. Until such guidance is issued, however, the planning guidance included in OMB Bulletin 90-08 can assist in determining techniques for effective security in a system and in addressing technical controls in the security plan.

g) System Interconnection. In order for a community to effectively manage risk, it must control access to and from other systems. The degree of such control should be established in the rules of the system and all participants should be made aware of any limitations on outside access. Technical controls to accomplish this should be put in place in accordance with guidance issued by NIST.

There are varying degrees of how connected a system is. For example, some systems will choose to isolate themselves, others will restrict access such as allowing only e-mail connections or remote access only with sophisticated authentication, and others will be fully open. The management decision to interconnect should be based on the availability and use of technical and non-technical safeguards and consistent with the acceptable

level of risk defined in the system rules.

3) Review of Security Controls. The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a deficiency.

4) Authorize Processing. The authorization of a system to process information, granted by a management official, provides an important quality control (some agencies refer to this authorization as accreditation). By authorizing processing in a system, a manager accepts the risk associated with it. Authorization is not a decision that should be made by the security staff.

Both the security official and the authorizing management official have security responsibilities. In general, the security official is closer to the day-to-day operation of the system and will direct or perform security tasks. The authorizing official will normally have general responsibility for the organization supported by the system.

Management authorization should be based on an assessment of management, operational, and technical controls. Since the security plan establishes the security controls, it should form the basis for the authorization, supplemented by more specific studies as needed. In addition, the periodic review of controls should also contribute to future authorizations. Some agencies perform "certification reviews" of their systems periodically. These formal technical evaluations lead to a management accreditation, or "authorization to process." Such certifications (such as those using the methodology in FIPS Pub 102 "Guideline for Computer Security Certification and Accreditation") can provide useful information to assist management in authorizing a system, particularly when combined with a review of the broad behavioral controls envisioned in the security plan required by the Appendix.

Re-authorization should occur prior to a significant change in processing, but at least every three years. It should be done more often where there is a high risk and potential magnitude of harm.

b. Controls in Major Applications. Certain applications require special management attention due to the risk and magnitude of harm that could occur. For such applications, the controls of the support system(s) in which they operate are likely to be insufficient. Therefore, additional controls specific to the application are

required. Since the function of applications is the direct manipulation and use of information, controls for securing applications should emphasize protection of information and the way it is manipulated.

1) Assign Responsibility for Security. By definition, major applications are high risk and require special management attention. Major applications usually support a single agency function and often are supported by more than one general support system. It is important, therefore, that an individual be assigned responsibility in writing to assure that the particular application has adequate security. To be effective, this individual should be knowledgeable in the information and process supported by the application and in the management, personnel, operational, and technical controls used to protect the application.

2) Application Security Plans. Security for each major application should be addressed by a security plan specific to the application. The plan should include controls specific to protecting information and should be developed from the application manager's perspective. To assist in assuring its viability, the plan should be provided to the manager of the primary support system which the application uses for advice and comment. This recognizes the critical dependence of the security of major applications on the underlying support systems they use. Summaries of application security plans should be included in strategic information resource management plans in accordance with this Circular.

a) Application Rules. Rules of behavior should be established which delineate the responsibilities and expected behavior of all individuals with access to the application. The rules should state the consequences of inconsistent behavior. Often the rules will be associated with technical controls implemented in the application. Such rules should include, for example, limitations on changing data, searching databases, or divulging information.

b) Specialized Training. Training is required for all individuals given access to the application, including members of the public. It should vary depending on the type of access allowed and the risk that access represents to the security of the application and information in it. This training will be in addition to that required for access to a support system.

c) Personnel Security. For most major applications, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. For example, technical controls to ensure individual accountability, such as looking for patterns of user behavior, are most effective if users are aware that there is such a technical control. If adequate audit or access controls (through both technical and non-technical methods) cannot be established, then it may be cost-effective to screen personnel, commensurate with the risk and magnitude of harm they could cause. The change in emphasis on screening in the Appendix should not affect background screening deemed necessary because of other duties that an individual may perform.

d) Contingency Planning. Normally the Federal mission supported by a major application is critically dependent on the application. Manual processing is generally NOT a viable back-up option. Managers should plan for how they will perform their mission and/or recover from the loss of existing application support, whether the loss is due to the inability of the

application to function or a general support system failure. Experience has demonstrated that testing a contingency plan significantly improves its viability. Indeed, untested plans or plans not tested for a long period of time may create a false sense of ability to recover in a timely manner.

e) Technical Controls. Technical security controls, for example tests to filter invalid entries, should be built into each application. Often these controls will correspond with the rules of behavior for the application. Under the previous Appendix, application security was focused on the process by which sensitive, custom applications were developed. While that process is not addressed in detail in this Appendix, it remains an effective method for assuring that security controls are built into applications. Additionally, the technical security controls defined in OMB Bulletin No. 90-08 will continue, until that guidance is replaced by NIST's security planning guidance.

f) Information Sharing. Assure that information which is shared with Federal organizations, State and local governments, and the private sector is appropriately protected comparable to the protection provided when the information is within the application. Controls on the information may stay the same or vary when the information is shared with another entity. For example, the primary user of the information may require a high level of availability while the secondary user does not, and can therefore relax some of the controls designed to maintain the availability of the information. At the same time, however, the information shared may require a level of confidentiality that should be extended to the secondary user. This normally requires notification and agreement to protect the information prior to its being shared.

g) Public Access Controls. Permitting public access to a Federal application is an important method of improving information exchange with the public. At the same time, it introduces risks to the Federal application. To mitigate these risks, additional controls should be in place as appropriate. These controls are in addition to controls such as "firewalls" that are put in place for security of the general support system.

In general, it is more difficult to apply conventional controls to public access systems, because many of the users of the system may not be subject to individual accountability policies. In addition, public access systems may be a target for mischief because of their higher visibility and published access methods.

Official records need to be protected against loss or alteration. Official records in electronic form are particularly susceptible since they can be relatively easy to change or destroy. Therefore, official records should be segregated from information made directly accessible to the public. There are different ways to segregate records. Some agencies and organizations are creating dedicated information dissemination systems (such as bulletin boards or World Wide Web servers) to support this function. These systems can be on the outside of secure gateways which protect internal agency records from outside access.

In order to secure applications that allow direct public access, conventional techniques such as least privilege (limiting the processing capability as well as access to data) and integrity assurances (such as checking for viruses, clearly labeling the age of data, or periodically spot checking data) should also be used. Additional guidance on securing public

access systems is available from NIST Computer Systems Laboratory Bulletin "Security Issues in Public Access Systems" (May, 1993).

3) Review of Application Controls. At least every three years, an independent review or audit of the security controls for each major application should be performed. Because of the higher risk involved in major applications, the review or audit should be independent of the manager responsible for the application. Such reviews should verify that responsibility for the security of the application has been assigned, that a viable security plan for the application is in place, and that a manager has authorized the processing of the application. A deficiency in any of these controls should be considered a deficiency pursuant to the Federal Manager's Financial Integrity Act and OMB Circular No. A-123, "Management Accountability and Control."

The review envisioned here is different from the system test and certification process required in the current Appendix. That process, however, remains useful for assuring that technical security features are built into custom-developed software applications. While the controls in that process are not specifically called for in this Appendix, they remain in Bulletin No. 90-08, and are recommended in appropriate circumstances as technical controls.

4) Authorize Processing. A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high. The intent of this requirement is to assure that the senior official whose mission will be adversely affected by security weaknesses in the application periodically assesses and accepts the risk of operating the application. The authorization should be based on the application security plan and any review(s) performed on the application. It should also take into account the risks from the general support systems used by the application.

4. Assignment of Responsibilities. The Appendix assigns government-wide responsibilities to agencies that are consistent with their missions and the Computer Security Act.

a. Department of Commerce. The Department of Commerce, through NIST, is assigned the following responsibilities consistent with the Computer Security Act.

1) Develop and issue security standards and guidance.

2) Review and update, with assistance from OPM, the guidelines for security training issued in 1988 pursuant to the Computer Security Act to assure they are effective.

3) Replace and update the technical planning guidance in the appendix to OMB Bulletin 90-08 This should include guidance on effective risk-based security absent a formal risk analysis.

4) Provide agencies with guidance and assistance concerning effective controls for systems when interconnecting with other systems, including the Internet. Such guidance on, for example, so-called "firewalls" is becoming widely available and is critical to agencies as they consider how to interconnect their communications capabilities.

5) Coordinate agency incident response activities. Coordination of agency incident response activities should address both threats and vulnerabilities as well as improve the ability of the Federal government for rapid and effective cooperation in response to serious security breaches.

6) Assess security vulnerabilities in new information technologies and apprise Federal agencies of such vulnerabilities. The intent of this new requirement is to help agencies understand the security implications of technology before they purchase and field it. In the past, there have been too many instances where agencies have acquired and implemented technology, then found out about vulnerabilities in the technology and had to retrofit security measures. This activity is intended to help avoid such difficulties in the future.

b. Department of Defense. The Department, through the National Security Agency, should provide technical advice and assistance to NIST, including work products such as technical security guidelines, which NIST can draw upon for developing standards and guidelines for protecting sensitive information in Federal computers.

Also, the Department, through the National Security Agency, should assist NIST in evaluating vulnerabilities in emerging technologies. Such vulnerabilities may present a risk to national security information as well as to unclassified information.

c. Department of Justice. The Department of Justice should provide appropriate guidance to Federal agencies on legal remedies available to them when serious security incidents occur. Such guidance should include ways to report incidents and cooperate with law enforcement.

In addition, the Department should pursue appropriate legal actions on behalf of the Federal government when serious security incidents occur.

d. General Services Administration. The General Services Administration should provide agencies guidance for addressing security considerations when acquiring information technology products or services. This continues the current requirement.

In addition, where cost-effective to do so, GSA should establish government-wide contract vehicles for agencies to use to acquire certain security services. Such vehicles already exist for providing system back-up support and conducting security analyses.

GSA should also provide appropriate security services to assist Federal agencies to the extent that provision of such services is cost-effective. This includes providing, in conjunction with the Department of Defense and the Department of Commerce, appropriate services which support Federal use of the National Information Infrastructure (e.g., use of digital signature technology).

e. Office of Personnel Management. In accordance with the Computer Security Act, OPM should review its regulations concerning computer security training and assure that they are effective.

In addition, OPM should assist the Department of Commerce in the review and update of its computer security awareness and training guidelines. OPM worked closely with NIST in developing the current guidelines and should work with NIST in revising those guidelines.

f. Security Policy Board. The Security Policy Board is assigned responsibility for

national security policy coordination in accordance with the appropriate Presidential directive. This includes policy for the security of information technology used to process classified information.

Circular A-130 and this Appendix do not apply to information technology that supports certain critical national security missions, as defined in 44 U.S.C. 3502(9) and 10 U.S.C. 2315. Policy and procedural requirements for the security of national security systems (telecommunications and information systems that contain classified information or that support those critical national security missions (44 U.S.C. 3502(9) and 10 U.S.C. 2315)) is assigned to the Department of Defense pursuant to Presidential directive. The Circular clarifies that information classified for national security purposes should also be handled in accordance with appropriate national security directives. Where classified information is required to be protected by more stringent security requirements, those requirements should be followed rather than the requirements of this Appendix.

5. Reports. The Appendix requires agencies to provide two reports to OMB:

The first is a requirement that agencies report security deficiencies and material weaknesses within their FMFIA reporting mechanisms as defined by OMB Circular No. A-123, "Management Accountability and Control," and take corrective actions in accordance with that directive.

The second, defined by the Computer Security Act, requires that a summary of agency security plans be included in the information resources management plan required by the Paperwork Reduction Act.

NATIONAL SECURITY PRESIDENTIAL DIRECTIVE-1

SUBJECT: Organization of the National Security Council System

This document is the first in a series of National Security Presidential Directives. National Security Presidential Directives shall replace both Presidential Decision Directives and Presidential Review Directives as an instrument for communicating presidential decisions about the national security policies of the United States.

National security includes the defense of the United States of America, protection of our constitutional system of government, and the advancement of United States interests around the globe. National security also depends on America's opportunity to prosper in the world economy. The National Security Act of 1947, as amended, established the National Security Council to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. That remains its purpose. The NSC shall advise and assist me in integrating all aspects of national security policy as it affects the United States -- domestic, foreign, military, intelligence, and economics (in conjunction with the National Economic Council (NEC)). The National Security Council system is a process to coordinate executive departments and agencies in the effective development and implementation of those national security policies.

The National Security Council (NSC) shall have as its regular attendees (both statutory and non-statutory) the President, the Vice President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, and the Assistant to the President for National Security Affairs. The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff, as statutory advisors to the NSC, shall also attend NSC meetings. The Chief of Staff to the President and the Assistant to the President for Economic Policy are invited to attend any NSC meeting. The Counsel to the President shall be consulted regarding the agenda of NSC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S.C. 511 to give his advice and opinion on questions of law when required by the President. The heads of other executive departments and agencies, as well as other senior officials, shall be invited to attend meetings of the NSC when appropriate.

The NSC shall meet at my direction. When I am absent from a meeting of the NSC, at my direction the Vice President may preside. The Assistant to the President for National Security Affairs shall be responsible, at my direction and in consultation with the other regular attendees of the NSC, for determining the agenda, ensuring that necessary papers are prepared, and recording NSC actions and Presidential decisions. When international economic issues are on the agenda of the NSC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these

tasks in concert.

The NSC Principals Committee (NSC/PC) will continue to be the senior interagency forum for consideration of policy issues affecting national security, as it has since 1989. The NSC/PC shall have as its regular attendees the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Chief of Staff to the President, and the Assistant to the President for National Security Affairs (who shall serve as chair). The Director of Central Intelligence and the Chairman of the Joint Chiefs of Staff shall attend where issues pertaining to their responsibilities and expertise are to be discussed. The Attorney General and the Director of the Office of Management and Budget shall be invited to attend meetings pertaining to their responsibilities. For the Attorney General, this includes both those matters within the Justice Department's jurisdiction and those matters implicating the Attorney General's responsibility under 28 U.S C. 511 to give his advice and opinion on questions of law when required by the President. The Counsel to the President shall be consulted regarding the agenda of NSC/PC meetings, and shall attend any meeting when, in consultation with the Assistant to the President for National Security Affairs, he deems it appropriate. When international economic issues are on the agenda of the NSC/PC, the Committee's regular attendees will include the Secretary of Commerce, the United States Trade Representative, the Assistant to the President for Economic Policy (who shall serve as chair for agenda items that principally pertain to international economics), and, when the issues pertain to her responsibilities, the Secretary of Agriculture. The Chief of Staff and National Security Adviser to the Vice President shall attend all meetings of the NSC/PC, as shall the Assistant to the President and Deputy National Security Advisor (who shall serve as Executive Secretary of the NSC/PC). Other heads of departments and agencies, along with additional senior officials, shall be invited where appropriate.

The NSC/PC shall meet at the call of the Assistant to the President for National Security Affairs, in consultation with the regular attendees of the NSC/PC. The Assistant to the President for National Security Affairs shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared. When international economic issues are on the agenda of the NSC/PC, the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy shall perform these tasks in concert.

The NSC Deputies Committee (NSC/DC) will also continue to serve as the senior sub-Cabinet interagency forum for consideration of policy issues affecting national security. The NSC/DC can prescribe and review the work of the NSC interagency groups discussed later in this directive. The NSC/DC shall also help ensure that issues being brought before the NSC/PC or the NSC have been properly analyzed and prepared for decision. The NSC/DC shall have as its regular members the Deputy Secretary of State or Under Secretary of the Treasury or Under Secretary of the Treasury for International Affairs, the Deputy Secretary of Defense or Under Secretary of Defense for Policy, the Deputy Attorney General, the Deputy Director of the Office of Management and Budget, the Deputy Director of Central Intelligence, the Vice Chairman of the Joint Chiefs of Staff, the Deputy Chief of Staff to the President for Policy, the Chief of Staff and National Security Adviser to the Vice President, the Deputy Assistant to the President for International Economic Affairs, and the Assistant to the President and Deputy National Security Advisor (who shall serve as chair). When international economic issues are on the agenda, the NSC/DC's regular membership will include the Deputy Secretary of Commerce, a Deputy United States Trade Representative, and, when the issues pertain to his responsibilities, the Deputy Secretary of

Agriculture, and the NSC/DC shall be chaired by the Deputy Assistant to the President for International Economic Affairs for agenda items that principally pertain to international economics. Other senior officials shall be invited where appropriate.

The NSC/DC shall meet at the call of its chair, in consultation with the other regular members of the NSC/DC. Any regular member of the NSC/DC may also request a meeting of the Committee for prompt crisis management. For all meetings the chair shall determine the agenda in consultation with the foregoing, and ensure that necessary papers are prepared.

The Vice President and I may attend any and all meetings of any entity established by or under this directive.

Management of the development and implementation of national security policies by multiple agencies of the United States Government shall usually be accomplished by the NSC Policy Coordination Committees (NSC/PCCs). The NSC/PCCs shall be the main day-to-day fora for interagency coordination of national security policy. They shall provide policy analysis for consideration by the more senior committees of the NSC system and ensure timely responses to decisions made by the President. Each NSC/PCC shall include representatives from the executive departments, offices, and agencies represented in the NSC/DC.

Six NSC/PCCs are hereby established for the following regions: Europe and Eurasia, Western Hemisphere, East Asia, South Asia, Near East and North Africa, and Africa. Each of the NSC/PCCs shall be chaired by an official of Under Secretary or Assistant Secretary rank to be designated by the Secretary of State.

Eleven NSC/PCCs are hereby also established for the following functional topics, each to be chaired by a person of Under Secretary or Assistant Secretary rank designated by the indicated authority:

Democracy, Human Rights, and International Operations (by the Assistant to the President for National Security Affairs);

International Development and Humanitarian Assistance (by the Secretary of State);

Global Environment (by the Assistant to the President for National Security Affairs and the Assistant to the President for Economic Policy in concert);

International Finance (by the Secretary of the Treasury);

Transnational Economic Issues (by the Assistant to the President for Economic Policy);

Counter-Terrorism and National Preparedness (by the Assistant to the President for National Security Affairs);

Defense Strategy, Force Structure, and Planning (by the Secretary of Defense);

Arms Control (by the Assistant to the President for National Security Affairs);

Proliferation, Counterproliferation, and Homeland Defense (by the Assistant to the President for National Security Affairs);

Intelligence and Counterintelligence (by the Assistant to the President for National Security Affairs); and

Records Access and Information Security (by the Assistant to the President for National Security Affairs).

The Trade Policy Review Group (TPRG) will continue to function as an interagency coordinator of trade policy. Issues considered within the TPRG, as with the PCCs, will flow through the NSC and/or NEC process, as appropriate.

Each NSC/PCC shall also have an Executive Secretary from the staff of the NSC, to be designated by the Assistant to the President for National Security Affairs. The Executive Secretary shall assist the Chairman in scheduling the meetings of the NSC/PCC, determining the agenda, recording the actions taken and tasks assigned, and ensuring timely responses to the central policymaking committees of the NSC system. The Chairman of each NSC/PCC, in consultation with the Executive Secretary, may invite representatives of other executive departments and agencies to attend meetings of the NSC/PCC where appropriate.

The Assistant to the President for National Security Affairs, at my direction and in consultation with the Vice President and the Secretaries of State, Treasury, and Defense, may establish additional NSC/PCCs as appropriate.

The Chairman of each NSC/PCC, with the agreement of the Executive Secretary, may establish subordinate working groups to assist the PCC in the performance of its duties.

The existing system of Interagency Working Groups is abolished.

- The oversight of ongoing operations assigned in PDD/NSC-56 to Executive Committees of the Deputies Committee will be performed by the appropriate regional NSC/PCCs, which may create subordinate working groups to provide coordination for ongoing operations.

- The Counter-Terrorism Security Group, Critical Infrastructure Coordination Group, Weapons of Mass Destruction Preparedness, Consequences Management and Protection Group, and the interagency working group on Enduring Constitutional Government are reconstituted as various forms of the NSC/PCC on Counter-Terrorism and National Preparedness.

- The duties assigned in PDD/NSC-75 to the National Counterintelligence Policy Group will be performed in the NSC/PCC on Intelligence and Counterintelligence, meeting with appropriate attendees.

- The duties assigned to the Security Policy Board and other entities established in PDD/NSC-29 will be transferred to various NSC/PCCs, depending on the particular security problem being addressed.

- The duties assigned in PDD/NSC-41 to the Standing Committee on Nonproliferation will be transferred to the PCC on Proliferation, Counterproliferation, and Homeland Defense.

- The duties assigned in PDD/NSC-35 to the Interagency Working Group for Intelligence Priorities will be transferred to the PCC on Intelligence and Counterintelligence.

- The duties of the Human Rights Treaties Interagency Working Group established in E.O. 13107 are transferred to the PCC on Democracy, Human Rights, and International Operations.

- The Nazi War Criminal Records Interagency Working Group established in E.O. 13110 shall be reconstituted, under the terms of that order and until its work ends in January 2002, as a Working Group of the NSC/PCC for Records Access and Information Security.

Except for those established by statute, other existing NSC interagency groups, ad hoc bodies, and executive committees are also abolished as of March 1, 2001, unless they are specifically reestablished as subordinate working groups within the new NSC system as of that date. Cabinet officers, the heads of other executive agencies, and the directors of offices within the Executive Office of the President shall advise the Assistant to the President for National Security Affairs of those specific NSC interagency groups chaired by their respective departments or agencies that are either mandated by statute or are otherwise of sufficient importance and vitality as to warrant being reestablished. In each case the Cabinet officer, agency head, or office director should describe the scope of the activities proposed for or now carried out by the interagency group, the relevant statutory mandate if any, and the particular NSC/PCC that should coordinate this work. The Trade Promotion Coordinating Committee established in E.O. 12870 shall continue its work, however, in the manner specified in that order. As to those committees expressly established in the National Security Act, the NSC/PC and/or NSC/DC shall serve as those committees and perform the functions assigned to those committees by the Act.

To further clarify responsibilities and effective accountability within the NSC system, those positions relating to foreign policy that are designated as special presidential emissaries, special envoys for the President, senior advisors to the President and the Secretary of State, and special advisors to the President and the Secretary of State are also abolished as of March 1, 2001, unless they are specifically redesignated or reestablished by the Secretary of State as positions in that Department.

This Directive shall supersede all other existing presidential guidance on the organization of the National Security Council system. With regard to application of this document to economic matters, this document shall be interpreted in concert with any Executive Order governing the National Economic Council and with presidential decision documents signed hereafter that implement either this directive or that Executive Order.

cc: The Executive Clerk

SafeGuard Program

Subscribing Parent Agency	Subscribing Sub-Agencies
Dept. of the Treasury	U.S. Customs
	Financial Management Service
	Bureau of Public Debt
	United States Secret Service
Dept. of Agriculture	
Dept. of Justice	
Dept. of the Interior	
Dept. of Health and Human Services	National Institutes of Health
	Center of Disease Control
Dept. of Defense	U.S. Army Reserve Command
	Military Sealift Command
	Air Force Materiel Command
	National Imagery and Mapping agency
Dept. of Transportation	Federal Aviation Administration
Office of Personnel Management	
Federal Emergency Management Agency	
Dept. of Veterans Affairs	Veteran's Health Administration
Federal Communications Commission	
General Services Administration	FTS FedCIRC
Dept. of Housing and Urban development	
Agreements in Processing	
U.S. Army Corps of Engineers	DOS Diplomatic Security
Supreme Court	Federal Bureau of Investigation
U.S. Geological Survey	U.S. Courts
Social Security Administration	United States Marine Corps

Profiles of Major Incidents

Below are profiles of three major incidents that occurred in 2000 and affected government agencies.

1. T0rn Rootkit

T0rnkit is a collection of files designed to replace portions of the operating system with the intent of providing a more suitable environment to intrude on other computers. It has features that obfuscate this installation, avoid authentication measures, and attack other computers. T0rnkit has been installed on thousands of computers worldwide, including several in US Government agencies. Four agencies have reported rootkit incidents. The extent of any damage from rootkit has not been reported to FedCIRC.

There is some evidence that this rootkit is of foreign origin, and foreign sites remain frequently identified in intrusion reports. The rootkit itself does not markedly interfere with operation of the computer, but it grants unauthorized privilege to intruders. There are multiple styles of intrusion that use this rootkit, showing differing levels of expertise on the part of the intruders, differing language abilities, and differing goals. This appears to be more of a "means to an end" than an end in itself, and as such bears close future examination.

2. Halloween Hack Attack

The "Halloween Hack Attack" was a mass web page defacement, which took place between September 6, 2000 and October 16, 2000. Ten U. S. Government domain web pages were defaced. The defacements were signed and messages were left on the affected web pages. No irreparable damage was done to the compromised machines.

3. Love Letter Malicious Code

"Love Letter" is a malicious program (categorized as a worm) which spreads in a variety of ways. FedCIRC received reports that indicated virtually all government sites suffered some related repercussions. Though many government sites did not propagate the love letter "worm," they still saw marked increase in the amount of incoming mail from external organizations and individuals that employed Microsoft Outlook as their mail client. Several government agencies and departments, in a panic response to the flood of email clogging their systems, chose to disconnect their networks from the Internet. This action did limit the propagation of the worm to some extent but it also prevented agencies from receiving critical information and solutions to the problem. In general, there were numerous reports of sites suffering considerable network degradation as a result of mail, file, and web traffic generated by the "love letter" malicious code.

Too much information
Too little time

50% OFF BESTSELLERS

ISSUE 2135 Friday 30 March 2001

Hacking 'is now bigger threat than terrorism'

By George Jones and Michael Smith

External Links

- Foreign & Commonwealth Office
- MI5 The Security Service
- Information Assurance Advisory Council
- Data security - Department of Trade & Industry
- Security News Network
- Internet firewalls and security - 3com
- Electronic Privacy Information Centre

COMPUTER hacking could now cripple Britain more quickly than a military strike or terrorist campaign, Robin Cook, the Foreign Secretary, told the Commons last night.

He said that the electronic technology controlling essential services such as water, power and transport had become a leading target for terrorists and other groups who wanted to disrupt the life of the nation.

Mr Cook gave a graphic account of how terrorists or anti-capitalist protesters could wreak havoc in a modern economy such as Britain's if they managed to gain access to the computer systems of the key public services.

Mr Cook said: "The revolution in communications technology is creating new opportunities on an exponential scale. This week, 360,000 e-mails will be sent in Britain every second, a fifth more than in January and twice as many as last June. Computers now manage most of our critical national infrastructure, but with these new opportunities there also comes the risk of new threats."

"A computer-based attack could cripple the nation more quickly than a military strike," Mr Cook told MPs during a debate on the work of the intelligence and security services.

Mr Cook said the intelligence services had also helped to stop Jamaican Yardies smuggling drugs into Britain. The spies' work had led to the seizure of major shipments of heroin and cocaine, as well as to the arrest of the drug traders involved and to the seizure of their assets.

Mr Cook said: "British agencies contributed to a recent operation in the Caribbean which resulted in a drugs haul worth £70 million, in just one raid."

The Foreign Secretary emphasised that the security service was adapting to new threats to national life following the thawing of East-West relations. Ministers are known to be concerned that anarchists and extreme Left-wing groups are threatening to disrupt the City of London with "anti-capitalist" demonstrations in May.

Last year, a demonstration by the anti-capitalist Reclaim the Streets group brought widespread disruption to the centre of London, with the statue of Winston Churchill in Parliament Square defaced by protesters and a McDonalds restaurant wrecked.

A year earlier, 6,000 demonstrators created chaos in the City of London. This year activists are planning to take over hotels, the offices of privatised utilities and streets "associated with capitalism".

Julian Lewis, the Conservative MP for New Forest East, said a serious mistake had been made when MI5's anti-subversion "F Branch" was, in effect, closed down. It was done in the belief that subversion in Britain was a "historical phenomenon" following the decline of extreme organisations on the Left and the Right.

Had it still been active the police would have had less trouble controlling the anti-capitalist demonstrations. Worse still, he added, it was not available to gather information on action being planned for May Day this year which could seriously disrupt a general election.

25 January 2001: [Connected] Security hole threatens UK e-tailers
2 November 2000: [Connected] Anti-hacking site falls to hacker
2 November 2000: [Connected] Microsoft humiliated as hackers crack Windows
10 August 2000: [Connected] Beijing hackers steal American nuclear secrets
2 May 2000: Blair condemns the 'mindless thugs' in May Day rampage
19 June 1999: Mobs put City under siege

▲ Return to top

Next UK Report ▸ DTI report on Maxwell highlights City errors

Search UK News ▸ ▸ Find

Front Page | UK News | International | Weather | Crosswords | Matt cartoon | Feedback
City News | City Analysis | Small Businesses | Personal Finance (Telegraph Money) | Alex cartoon

WHITE PAPER

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63

May 22, 1998

WHITE PAPER
The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63
May 22, 1998

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.

II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;

- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.

- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.

- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.

- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available as appropriate, to ensure that critical infrastructure protection is achieved and maintained.

- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.

- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.

- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.

- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.

3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure

Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.

4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.

2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.

3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.

4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.

5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.

7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.

8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.

9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.

10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.

Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National

Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan Coordination (NPC) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The NPC staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The NPC staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the NPC, during the remainder of FY98. Beginning in FY99, the NPC shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the NPC's operations. The NPC will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the

National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.

Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.

- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.

- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.

- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.

- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.

- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.

Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.

- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.

- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.

- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.

- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.

- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.

- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.

- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based

systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.

- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.

- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.

- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.

- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.

Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.

- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.

- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.

FedCIRC Incident Activity Summary for 2000

A total of **586 incidents** were reported to FedCIRC during the period January through December 2000. The reported incidents had potential impact on **575,568 hosts** in the **.GOV** domain.

Summary of report types

Count	Percentage	Type
155	26%	Root compromise
113	19%	User account compromise
70	11%	Network Reconnaissance
36	6%	Virus/Worm
35	5%	Denial of service
24	4%	Misuse of resources
24	4%	False alarm
9	1%	Unknown or Unidentifiable
7	1%	Deception
138	23%	Information request

Note:

- The number of reported incidents reflected in the table above exceed the total number of reports received. Incidents often fall into multiple categories.
- Requests for security related information or assistance are recorded as incident reports if received through e-mail, Fax or telephone.

Current FedCIRC Incident Activity Summary (January 2001 to Present)

During the period **Jan 2001 to date**, 67 reports have been received of defacements to government web sites. Of those reported, several were repeat defacements, exploiting commonly known vulnerabilities for which, security solutions are readily available.

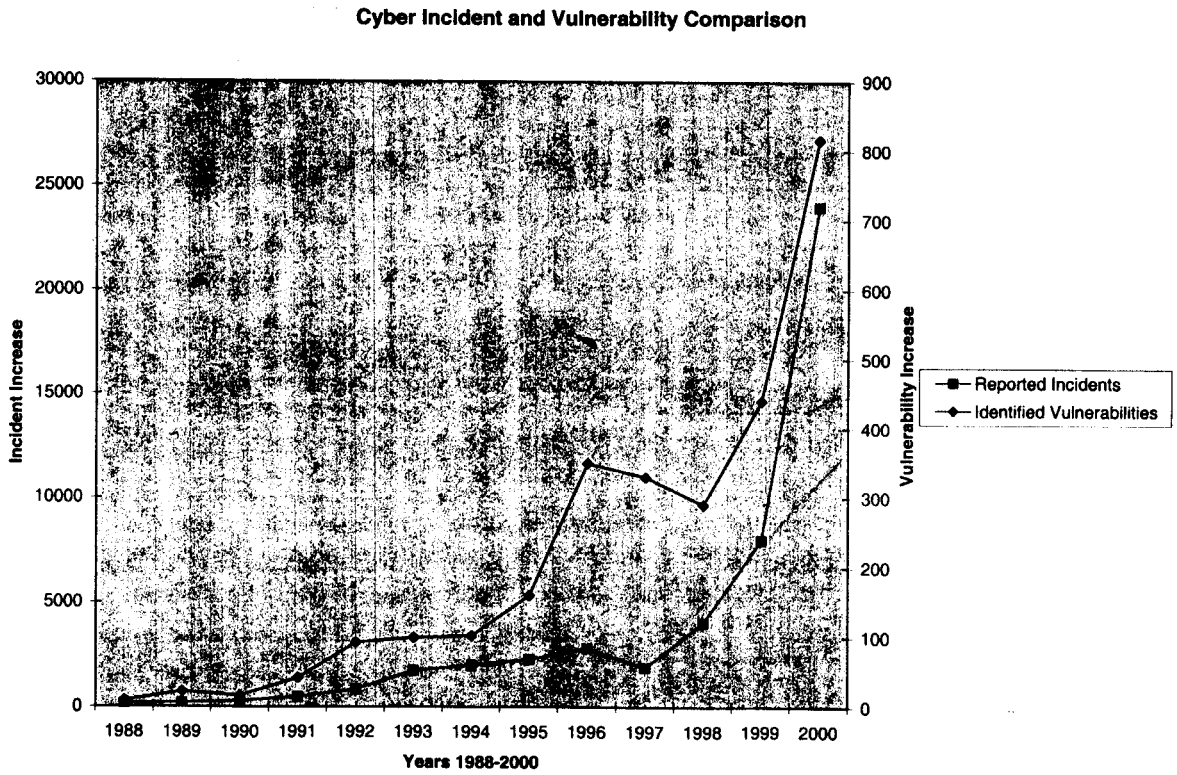
19 of the 67 defacements reported during this period occurred between March 16-19, 2001. All hosts involved were Windows NT or Windows 2000 platforms. A single perpetrator (***"PoizonBox"***) claimed responsibility for all but one of the defacements. FedCIRC is currently collecting log data from the affected agencies to further analyze the incident and identify the particular exploit. The only evidence at this point in our investigation implicates a host residing in Estonia but assumptions are that this was another compromised system being used unknowingly in the attack.

During the month of March, 26 new viruses were detected in the wild. Of the 26 detected, only one was judged to be a significant threat.

134 incidents have been reported to FedCIRC since the beginning of the calendar year impacting 7467 government hosts.

Cumulative Incident Summary (January 2001 to Present)

Count	Percentage	Type
42	37.5%	Root compromise
33	29.5%	User account compromise
12	10.7%	Network Reconnaissance
11	9.8%	Virus/Worm
3	2.6%	Denial of service
1	0.8%	Misuse of resources
1	0.8%	False alarm
1	0.8%	Deception
7	6.2%	Information request
1	0.8%	Hoax


Cyber Incident and Vulnerability Comparison
Incident Increase
30000
25000
20000
15000
10000
5000
0
Vulnerability Increase
900
800
700
600
500
400
300
200
100
0
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
Years 1988-2000
Reported Incidents
Identified Vulnerabilities

EXCERPTS
OF

PCIE/ECIE Review Guide
Phase I

For use in reviewing an agency's

Critical Infrastructure Assurance Program

December 15, 1999

Prepared by: Office of Inspector General
National Aeronautics and Space Administration

Review Guide -- Table of Contents

I.	Introduction	1
II.	Objectives, Scope, and Methodology	2
III.	Acronyms	3
IV.	Special Instructions	3
V.	Criteria	4
VI.	Recent Audits	5
VII.	Milestones for Phases I through IV	5
VIII.	Review Steps	6
	General Steps	6
	Specific Steps	6
	A. Critical Infrastructure Planning	6
	B. Identification of Critical Assets	9
	C. Vulnerability Assessments	10
Appendix 1	Phase (Tier) I and II Agencies	12
Appendix 2	Model Role for the Inspector General in Critical Infrastructure Assurance	13
Appendix 3	Schedule of Review Results	14

VIII. Review Steps (Note: Steps apply only to critical cyber-based infrastructures)

General Steps

Objectives. *Identify past and present issues related to the agency's critical infrastructure, and the criteria and management roles and responsibilities related to its critical infrastructure. (These steps are intended to help identify work previously performed by your agency and to avoid unnecessary duplication of review effort. File the results with your working papers.)*

1. Identify agency internal and external management reports related to critical infrastructure. If recommendations were made in these reports, determine the status of actions taken to implement the recommendations.

2. Familiarize yourself with the criteria and organizational structure that your agency uses to manage its critical infrastructure.
   a. Identify the organization(s) in the agency having responsibility for interpreting Federal critical infrastructure guidance and developing agency infrastructure policies, procedures, and standards.
   b. Determine whether the agency has formalized its critical infrastructure protection (CIP) standards, policies, and procedures.

Specific Steps.[1] After an agency has established its critical infrastructure protection plans and policy, it should identify critical assets relevant to PDD 63, identify and analyze critical asset infrastructure dependencies and interdependencies, and conduct appropriate vulnerability assessments.

A. Critical Infrastructure Planning

Objective: *Determine whether departments and agencies*[2] *have developed an effective plan for protecting their critical cyber-based infrastructures.* ***Note: Answer all questions that follow on the Schedule of Review Results (Appendix 3). All "no" answers require information on the cause, effect, resolution, cost, and recommendation, when applicable.***

1. Has the agency completed its critical infrastructure protection plan (CIPP)? If no, determine when your agency plans to complete the CIPP.

2. If the agency does not plan to complete a CIPP, is it because the agency was not included among the Phase I and Phase II agencies specifically subject to PDD 63? (A list of Phase I/II agencies is provided in Appendix 1.)

3. If the answer to question A.2. is yes, then identify some of your agency's cyber-based assets that may be subject to PDD 63. (The White Paper for PDD 63 defines critical infrastructures as those

[1] Sources of information used to compile the general review guidance included the *White Paper - - The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63*; NASA's draft *Critical Infrastructure Protection Plan*, dated January 1999; and the draft National Plan for Information System Protection, dated Setpember16, 1999.
[2] To simplify, departments and agencies are hereafter referred to as agencies

physical and cyber-based systems essential to the minimum operations of the economy and government.) For the cyber-based assets so identified, does agency management agree that any of them should be subject to PDD 63? Note: For those OIG's that answered question A.3., please submit the schedule and summary of review results for work performed through this step. Your participation in this review is then finished.

4. For those agencies that have prepared a CIPP, did the Critical Infrastructure Coordination Group sponsor an "expert review process" for the CIPP, as required? (If yes, obtain a copy of the Expert Review Team (ERT) results for your agency. Refer to the applicable ERT results when performing the remaining steps in this Review Guide. If an ERT review was not performed, then determine the "cause" and continue with the remaining steps.

5. If the Critical Infrastructure Coordination Group has completed the expert review and found the CIPP deficient, has the agency taken adequate remedial action(s)?

6. Does the CIPP require the appointment of a Chief Infrastructure Assurance Officer (CIAO) who will have overall responsibility for protecting the agency's critical infrastructure?

7. Has the agency appointed a CIAO?

8. Does the CIPP require the agency to identify its cyber-based MEI?

9. Does the CIPP identify a milestone for identifying its cyber-based MEI?

10. Does the agency CIPP require an evaluation of new assets to determine whether they should be included in its MEI?

11. Does the CIPP require the agency to perform vulnerability assessments of its cyber-based MEI?

12. Does the CIPP require periodic updates of the assessments?

13. Does the CIPP identify milestones for completing the vulnerability assessments?

14. Does the CIPP require risk mitigation relative to potential damage stemming from each vulnerability?

15. Does the CIPP provide for periodic testing and re-evaluation of risk mitigation steps (policies, procedures, and controls) by agency management?

16. Does the CIPP provide a milestone for taking steps to mitigate risks?

17. Does the CIPP require establishment of an emergency management program?

18. If the answer to number 17 is yes, does the CIPP specify that the emergency management program include:

a. Incorporation of indications and warnings?
b. Incident collection, reporting, and analysis?
c. Response and continuity of operation plans?
d. A system for responding to significant infrastructure attacks, while the attacks are underway, with the goal of isolating and minimizing damage?
e. Notification to OIG criminal investigators of infrastructure attacks?

19. Does the CIPP require establishment of a system for quickly reconstituting minimum required capabilities following a successful infrastructure attack?

20. Does the CIPP identify a milestone for establishing the emergency management program?

21. Does the CIPP require a review of existing policies and procedures to determine whether the agency should revise them to reflect PDD 63 requirements?

22. Does the CIPP identify a milestone for reviewing existing policies and procedures?

23. Does the CIPP require the agency to ensure that security planning procedures are being incorporated into the basic design of new programs that include critical infrastructures, including provisions for:

a. Risk management and assessments?
b. Security plans for IT systems?
c. Security for command, control, and communications?
d. Identification of classified or sensitive information?
e. Awareness and training measures to be taken for each program?

24. Does the CIPP identify a milestone for establishing procedures to ensure that the agency incorporates security planning into the basic design of new programs?

25. Does the CIPP require the agency to incorporate its CIP functions into its strategic planning and performance measurement frameworks?

26. Does the CIPP identify a milestone for incorporating its critical infrastructure protection functions into its strategic planning and performance measurement frameworks?

27. Does the CIPP require agencies to identify resource and organizational requirements for implementing PDD 63?

28. Does the CIPP identify a milestone for identifying resource and organizational requirements for implementing PDD 63?

29. Does the CIPP require the agency to establish a program to ensure that it has the personnel and skills necessary to implement a sound infrastructure protection program?

30. Does the CIPP identify a milestone for establishing a program that would ensure the agency has the personnel and skills necessary to implement a sound infrastructure protection program?

31. Does the CIPP require the agency to establish effective CIP coordination with other applicable entities (foreign, state and local governments, and industry)?

32. Does the CIPP identify a milestone for establishing effective CIP coordination with other applicable entities (foreign, state and local governments, and industry)?

33. Do the agency's plans for the continuous/periodic review of its threat environment appear adequate, and is the agency complying with these plans?

B. Identification of Critical Assets

Objective. *Determine whether agencies have identified their cyber-based MEI and interdependencies.*[3]

1. Has the agency identified the following cyber-based MEI:
   a. People? (Staff, management - - including security management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission.)
   b. Technology? (All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.)
   c. Applications? (All application systems, internal and external, utilized in support of the core process.)
   d. Data? (All data - - electronic and hard copy - - and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or input into a computer, stored and processed there, or transmitted on some digital/communication's channel.)
   e. Facilities? (All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above in question B.1.)

2. Were the criteria used by the agency to identify its MEI consistent with the criteria used by the CIAO to identify agency MEI? (See footnote 1, page 1, for CIAO definition of agency MEI.)
   Added step: B2a. Did your agency use the CIAO infrastructure asset evaluation survey to identify its MEI assets?

3. Evaluate the adequacy of the agency's efforts to identify MEI and MEI interdependencies with applicable Federal agencies, state and local government activities, and industry.
   a. Has the agency identified assets consistent with the MEI as defined in question B.2?
   b. Did the agency use the results of itsYear 2000 (Y2K) work in identifying the MEI?

[3] Interdependence is defined by the National Plan for Information Systems Protection as "Dependence among elements or sites of different infrastructures, and therefore, effects by one infrastructure upon another."

c. Did the asset identification process include a determination of its estimated replacement costs, planned life cycle, and potential impact to the agency if the asset is rendered unusable?
d. Has the agency established milestones for identifying and reviewing their MEI?
e. Is the agency meeting its milestones?

C. Vulnerability Assessments

***Objective**. Determine whether agencies have adequately (1) identified the threats, vulnerabilities and potential magnitude of harm to their cyber-based MEI that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of the their critical cyber-based infrastructure investments, and (2) developed remediation plans to address the risks identified.*

Background: A vulnerability assessment is a systematic examination of the ability of a system or application, including current security procedures and controls, to withstand assault. Agencies can use vulnerability assessments to identify weaknesses that could be exploited and to predict the effectiveness of additional security measures in protecting information resources from attack.

The vulnerability assessment reviews actions, devices, policies, procedures, techniques, and other factors that potentially place an agency's critical asset elements at risk. The outcome of the assessment is a list of flaws or omissions in controls (vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or availability of resources that are essential to critical assets.

Gathering reliable information to perform vulnerability assessments requires teams of security specialists to perform structured interviews and to review all the written documents available for each area of control and each critical asset element.

1. Has the agency performed and documented an initial vulnerability assessment and developed remediation plans for its MEI?

2. Did the vulnerability assessments address the threat type and magnitude of the threat, the source of the threats, existing protection measures, the probability of occurrence, damage that could result from a successful attack, and the likelihood of success if such an attack occurred?

3. Did the remediation plans address the vulnerabilities found during the assessment?

4. Has the agency determined the level of protection currently in place for its MEI?

5. Has the agency identified the actions that must be taken before it can achieve a reasonable level of protection for its MEI?

6. If your answer to number 5 is yes, then has the agency developed a related implementation plan and mechanism to monitor such implementation?

7. Has the agency delegated responsibility for vulnerability assessments to the agency CIO?

8. Has the agency adopted a multi-year funding plan that addresses the identified threats?

9. Has the agency reflected the cost of implementing a multi-year vulnerability remediation plan in its FY 2001 budget submission to OMB?

10. Did the vulnerability assessments query national threat guidance for international, domestic, and state-sponsored terrorism/information warfare (e.g., from the Department of Defense, FBI, NSA, and other Federal and State agencies)?

11. Has the agency prioritized the threats according to their relative importance?

12. Has the agency assessed the vulnerability of its MEI to failures that could result from interdependencies with applicable Federal agencies, state and local government activities, and private sector providers of telecommunications, electrical power, and other infrastructure services?

13. Do the processes used to identify and reflect new threats to the agency's MEI appear adequate?

14. Do the results of the vulnerability assessments necessitate revisions to agency policies that govern the management and protection of agency MEI?

15. Did the results of the ERT coincide with answers derived from questions A.1 through C.14?

Schedule of Review Results

Agency: _____

OIG point of contact
Name: _____
Telephone No.: _____
E-mail address: _____

W/P Ref.	Review Step	Answer to Review Step: Yes	No	Not Applic.	Cause If "No" Answer in Col. (d)	Effect of Nonperformance	Est. Date of Resolution	Est. Cost of Resolution	Is Est. cost in Agency CIP Budget	Recommendation
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)	(k)
C-19	*Sample: A.15.d* Has the agency established a system for responding to significant infrastructure attacks while they are underway, with the goal of isolating and minimizing damage?		X		Agency has not designated an entity with responsibility for establishing such a system.	Ongoing damage may not be isolated and minimized. Ability to accomplish core mission may be severely harmed.	12/31/2000	No cost. Existing personnel will be used to prepare and implement the system.	Not applicable	Agency management should designate an entity with the responsibility for estabishing such a system.

Notes:
A mark in column (c) indicates that the agency has taken sufficient action.
A mark in column (d) indicates that the agency has not taken sufficient action.
Complete columns (f) through (k) only if column (d) has been marked.
Information contained in columns (h) and (i) should be obtained from the appropriate agency officials, not generated by the reviewer.