AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

HOW SECURE IS SENSITIVE COMMERCE DEPARTMENT DATA AND OPERATIONS? A REVIEW OF THE DEPARTMENT'S COMPUTER SECURITY POLICIES AND PRACTICES

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON ENERGY AND
COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SEVENTH CONGRESS

FIRST SESSION

AUGUST 3, 2001

Serial No. 107–56

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

74–853CC 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:

Bodman, Hon. Samuel W., Deputy Secretary, accompanied by Thomas Pyke, Acting Chief Information Officer, U.S. Department of Commerce . 40

Dacey, Robert F., Director, Information Security Issues, U.S. General Accounting Office 20

Frazier, Hon. Johnnie E., Inspector General, U.S. Department of Commerce 10

HOW SECURE IS SENSITIVE COMMERCE DEPARTMENT DATA AND OPERATIONS? A REVIEW OF THE DEPARTMENT'S COMPUTER SECURITY POLICIES AND PRACTICES

FRIDAY, AUGUST 3, 2001

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

The subcommittee met, pursuant to notice, at 9:30 a.m., in room 2123, Rayburn House Office Building, Hon. James C. Greenwood (chairman) presiding.

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

Staff present: Tom Dilenge, majority counsel; Mark Paoletta, majority counsel; Will Carty, legislative clerk; and Peter Kielty, legislative clerk.

Mr. GREENWOOD. Good morning. The subcommittee will come to order.

I apologize for starting a little late. It was a late night last night, and we are hoping some of the other members arrive, but we do not want to dishonor anyone's time. So we will start now.

We are here today to continue the committee's review of computer security, or lack thereof, as the case may be, at Federal agencies under our jurisdiction. Since 1998, this committee has reviewed computer security policies and practices at the Environmental Protection Agency, the Department of Energy, the Health Care Financing Administration, and today we will be focusing our attention on the Department of Commerce.

Without exception, we have found significant security problems at each of these agencies, all of which either took or are taking prompt action to correct the deficiencies identified as a result of our oversight.

Unfortunately, it appears that information security rarely becomes a priority within an agency until the white hot lights of public and congressional attention focus on that agency's specific flaws.

Today we will hear from information security experts at the General Accounting Office, who at this committee's request conducted an in depth evaluation of the department's management and implementation of computer security at seven of its operating divisions, including the Bureau of Export Administration, the International Trade Administration, the Economics and Statistics Administration, and the Office of the Secretary.

GAO's team of ethical hackers identified and exploited vulnerabilities in the computer systems of these divisions to gain virtually unlimited access to them internally from within the department's network and externally from the Internet.

Not only could these systems be accessed without authorization, but the information contained in them could be read, modified, or deleted at will, even with respect to the most sensitive systems and data files within these seven divisions.

And with such access also comes the power to completely disrupt critical department operations. It is no secret that of the systems reviewed and found to be vulnerable by GAO, many contain highly sensitive personal, financial, commercial, and national security related data and are critical to the department's overall mission.

Included in this list are the export control licensing systems and the networks that are used by the International Trade Administration for communications with our foreign commerce outposts around the world.

The state of the department's security was truly deplorable. GAO found instances in which systems did not require passwords even for system administrator accounts. Other systems had easily guessed passwords, such as "password."

Certain passwords and password files were either unencrypted or not otherwise protected, permitting anyone on the network, authorized or unauthorized, to read and obtain even the most powerful account passwords.

And six of the seven bureaus did not even limit the number of times an individual could try to log onto the system, allowing would be hackers excessive opportunities to crack these poor password controls.

GAO also found that poor network security and configurations permitted GAO's experts to circumvent the limited security controls that were in place and thus, to travel between and among the seven connected bureaus, essentially finding that the lowest common denominator among these bureaus set the security standard for the rest of them.

Some of the bureaus did not even have firewalls in place to protect all of their sensitive internal systems from the Internet or, if they did, they were either so poorly implemented as to be largely ineffective or could be easily bypassed by alternative access routes.

These failures place all of the connected bureaus at significant risks of intrusions.

Equally troubling, and despite advanced notice of the GAO hacking attempts, the department's monitoring of cyber intrusions failed to detect the overwhelming majority of GAO's intrusion and scanning efforts, including the successful ones.

In fact, GAO reports that its hackers gained access to one system only to find that a Russian hacker had been there before them without the department's apparent knowledge. And only two of the bureaus reviewed by GAO had formal intrusion detection systems in place.

In short, the department simply has no idea of whether its sensitive systems are being or have been compromised, a totally unacceptable situation.

The reason for these failures, according to GAO, is the lack of an effective security management program at the department. Basic and longstanding Federal security requirements have essentially been ignored for years. Only 3 of the 94 sensitive systems reviewed by GAO had documented risk assessments, and only seven had current security plans, none of which have been approved yet by management.

The department's computer security policies have not been updated since 1995, despite the tremendous growth of the Internet and the increased interconnectivity between Commerce bureaus and the outside world, and there are virtually no minimum security requirements for all Commerce computer systems, even, for example, on basic issues such as password lengths or characteristics.

In addition to GAO, we will hear today from the department's Inspector General, which also has done work in this area. A recent IG report essentially confirmed that the lack of effective security management found by GAO with respect to seven of the department's operating divisions was not unusual.

Across the department adequate risk assessments and security plans are the exception rather than the norm with roughly 92 percent of the department's systems failing to comply with at least one of these Federal security requirements.

The IG's financial control audits, which beginning this year contained a limited penetration test of computer security controls, also confirm that access control problems similar to those identified at the seven bureaus reviewed by GAO exist at many other Commerce bureaus as well, including the Census Bureau, NOAA, NIST, and others, posing threats from both internal and external sources.

How could this situation exist and for so long? The short answer is that until this committee started asking questions early last year, no one at the department was even seriously looking at these issues.

Despite Federal requirements for independent reviews of security controls on major systems on a routine basis, GAO found that neither the department's Chief Information Officer nor six of the seven bureaus reviewed had conducted any such audits or oversight.

Unfortunately the situation is not at all unusual. Our cyber security reviews have consistently shown that this lack of real world testing of the effectiveness of security controls is one of the major problems facing not just the Commerce Department, but the Federal Government as a whole.

This lack of attention to cyber security is reflected by the lack of resource devoted to this purpose. At Commerce, for example, the department's Office of Information Technology Security, which is responsible for setting the department's computer security policies and conducting oversight to insure compliance by these various bureaus, was a one-person operation until March 2000, when the Director of this office was given two interns to assist with these important functions.

I am pleased to hear that Secretary Evans recently approved a redirection of additional personnel and funding for this office, which in addition to computer security is also responsible for the department's overall critical infrastructure protection efforts.

It certainly is time; indeed, it is well past time for the Commerce Department to start taking the security of its data system seriously, much more so than it was under the previous administration.

In the 21st Century effective computer security is as much a part and cost of doing business as having locks on the front was during previous centuries. And we will continue our oversight in this area until Commerce and the other Federal agencies under our jurisdiction get this message loud and clear.

I want to welcome and thank our witnesses for testifying today on this important topic, and we'll now recognize the Ranking Member.

Actually, I will now recognize the chairman of the full committee, Mr. Tauzin, for his opening statement.

[The prepared statement of Hon. James Greenwood follows:]

PREPARED STATEMENT OF HON. JAMES GREENWOOD, CHAIRMAN, SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

We are here today to continue this Committee's review of computer security—or lack thereof as the case may be—at Federal agencies under our jurisdiction. Since 1998, this Committee has reviewed computer security policies and practices at the Environmental Protection Agency, the Department of Energy, the Health Care Financing Administration, and today we will be focusing our attention on the Department of Commerce. Without exception, we have found significant security problems at each of these agencies, all of which either took—or are taking—prompt action to correct the deficiencies identified as a result of our oversight. Unfortunately, it appears that information security rarely becomes a priority within an agency until the white-hot lights of public and congressional attention focus on that agency's specific flaws.

Today we will hear from information security experts at the General Accounting Office who, at this Committee's request, conducted an in-depth evaluation of the Department's management and implementation of computer security at seven of its operating divisions, including the Bureau of Export Administration, the International Trade Administration, the Economics and Statistics Administration, and the Office of the Secretary.

GAO's team of ethical hackers identified and exploited vulnerabilities in the computer systems of these divisions to gain virtually unlimited access to them internally, from within the Department's network, and externally, from the Internet. Not only could these systems be accessed without authorization, but the information contained in them could be read, modified, or deleted at will—even with respect to the most sensitive systems and data files within these seven divisions. And with such access also comes the power to completely disrupt critical Department operations.

It is no secret that, of the systems reviewed and found to be vulnerable by GAO, many contain highly sensitive personal, financial, commercial, and national security-related data, and are critical to the Department's overall mission. Included in this list are the export control licensing systems and the networks that are used by the International Trade Administration for communications with our foreign Commerce outposts around the world.

The state of the Department's security was truly deplorable. GAO found instances in which systems did not require passwords, even for system administrator accounts. Other systems had easily guessed passwords, such as "password." Certain passwords and password files were either unencrypted or not otherwise protected, permitting anyone on the network—authorized or unauthorized—to read and obtain even the most powerful account passwords. And six of the seven bureaus did not even limit the number of times an individual could try to log on to the system, allowing would-be hackers excessive opportunities to crack these poor password controls.

GAO also found that poor network security and configurations permitted GAO's experts to circumvent the limited security controls that were in place, and thus to travel between and among the seven connected bureaus—essentially finding that the lowest common denominator among these bureaus set the security standard for the rest of them. Some of the bureaus did not even have firewalls in place to protect all of their sensitive internal systems from the Internet—or, if they did, they were

either so poorly implemented as to be largely ineffective, or could be easily bypassed via alternative access routes. These failures place all of the connected bureaus at significant risk of intrusions.

Equally troubling, and despite advance notice of the GAO hacking attempts, the Department's monitoring of cyber intrusions failed to detect the overwhelming majority of GAO's intrusion and scanning efforts, including the successful ones. In fact, GAO reports that its hackers gained access to one system, only to find that a Russian hacker had been there before them, without the Department's apparent knowledge. And only two of the bureaus reviewed by GAO had formal intrusion detection systems in place. In short, the Department simply has no idea of whether its sensitive systems are being or have been compromised—a totally unacceptable situation.

The reason for these failures, according to GAO, is the lack of an effective security management program at the Department. Basic and longstanding Federal security requirements have essentially been ignored for years. Only *three* of the 94 sensitive systems reviewed by GAO had documented risk assessments, and only *seven* had current security plans, none of which had been approved yet by management. The Department's computer security policies have not been updated since 1995, despite the tremendous growth of the Internet and the increased inter-connectivity between Commerce bureaus and the outside world. And there are virtually no minimum security requirements for all Commerce computer systems—even, for example, on basic issues such as password lengths or characteristics.

In addition to GAO, we will hear today from the Department's Inspector General, which also has done work in this area. A recent IG report essentially confirmed that the lack of effective security management found by GAO, with respect to seven of the Department's operating divisions, was not unusual. Across the Department, adequate risk assessments and security plans are the exception rather than the norm, with roughly 92% of the Department's systems failing to comply with at least one of these Federal security requirements.

The IG's financial control audits, which, beginning this year, contained a limited penetration test of computer security controls, also confirm that access control problems similar to those identified at the seven bureaus reviewed by GAO exist at many other Commerce bureaus as well, including the Census Bureau, NOAA, NIST, and others, posing threats from both internal and external sources.

How could this situation exist, and for so long? The short answer is that, until this Committee started asking questions early last year, no one at the Department was even seriously looking at these issues. Despite Federal requirements for independent reviews of security controls on major systems on a routine basis, GAO found that neither the Department's chief information officer, nor six of the seven bureaus reviewed, had conducted any such audits or oversight.

Unfortunately, this situation is not at all unusual. Our cyber security reviews have consistently shown that this lack of real-world testing of the effectiveness of security controls is one of the major problems facing not just the Commerce Department, but the Federal government as a whole.

This lack of attention to cyber security is reflected by the lack of resources devoted to this purpose. At Commerce, for example, the Department's Office of Information Technology Security—which is responsible for setting the Department's computer security policies and conducting oversight to ensure compliance by the various bureaus—was a one-person operation up until March 2000, when the director of this office was given two interns to assist with these important functions. I am pleased to hear that Secretary Evans recently approved a re-direction of additional personnel and funding for this office, which in addition to computer security is also responsible for the Department's overall critical infrastructure protection efforts.

It certainly is time—indeed, it is well past time—for the Commerce Department to start taking the security of its data systems seriously, much more so than it was under the previous Administration. In the 21st century, effective computer security is as much a part and cost of doing business as having locks on the front door was during previous centuries. And we will continue our oversight in this area until Commerce and the other Federal agencies under our jurisdiction get this message loud and clear.

I want to welcome and thank our witnesses for testifying today on this important topic, and will now recognize the Ranking Member for an opening statement.

Chairman TAUZIN. Thank you, Mr. Chairman.

And let me echo your comments regarding the need for Federal agencies to start devoting a great deal more attention and re-

sources necessary to secure the computer systems of our country safe from the attacks or misuse from hackers.

I want to congratulate you, Jim, on the excellent work you have done as our O&I chairman this year, and this, of course, may be some of the most important work you do, even ranking with the important work you have done in tire safety this year to protect Americans.

Protecting the security of our systems is critical not only to the privacy of American citizens, who share information with these systems very often involuntarily, but they do not even have a chance to say, "Please do not use it for something else," but it obviously has huge implications for the potential for someone to create some real mischief in some very sensitive data banks in this country.

What we learned about the capability of hackers to move into, for example, CMS, (Center for Medicaid/Medicare Services) the agency formerly known as HCFA (Health Care Financing Administration), and interfere with the provision of health care services and reimbursement, sensitive medical accounts, it is pretty frightening.

You know, there is one area where citizens are keenly aware of the privacy of their information and the sanctity of that privacy. It is in the health care area.

I cannot tell you how appalled I was to learn that that information might be compromised and that the systems that my mother and so many other Americans depend upon for their health care might be ripped because somebody got in and managed it improperly and misused it.

And so again, I want to stress how important it is. This subcommittee has been moving on this issue, and again, Mr. Chairman, I congratulate you.

The Commerce Department, which is the focus of our hearing today, the GAO and Inspector General audit findings are alarming. Hackers from GAO and the Inspector General's Office were able to have their way with the department's various computer systems, violating the integrity of the department's computer networks virtually at will.

You know, if our government ethical hackers can get in, I guarantee you there are kids in Russia and Cal Tech, somewhere all over this world who can get in.

And while the findings are quite troubling, they don't surprise me based upon the committee's work on other agencies. When an administration, like the last administration, devotes so little time and attention to this particular matter, we are not surprised that these problems are so pervasive.

It is clear to me that while the former President might have said that this was an area of importance, the administration simply failed constantly, consistently to make the protection of our Nation's critical cyber assets a true priority. There just was not enough attention paid to it.

Somebody was asleep at the computer switch, and that is why I am pleased to see the new Secretary of Commerce is taking a very different approach.

He has instituted a new management structure with increased authority, responsibility, and accountability for the department's

information officers, and he has allocated more resources to the security functions at the departmental level.

And probably most importantly, the Secretary has made clear to his Under Secretaries that they will make computer security a priority as an integral part of their programmatic missions and will allocate additional resources as necessary to get the job done.

Those are strong words. We have heard strong words before. So we want to make sure those strong words are translated today and hereafter into very strong action.

In this vein I'm very pleased to have the newly confirmed Deputy Secretary of the department here today, signifying, I think, the importance of this topic to the Secretary and the level at which these issues are now being handled by the department. That is very encouraging.

Let me just finish by emphasizing that good computer security is not a simple fix. We have learned that in this committee. It is sort of like the radar systems, you know. For every new radar system they manufacture for the police, the same company is manufacturing a radar detection system for consumers to put in their cars.

And we know that the people who make the best security systems also know how to break them, and very often the people that are really good at this stuff figure it out on their own.

And while it takes consistent and sustained leadership, particularly in the beginning, effective long-term information security programs require their implementation, sound processes and policies that can carry on absent or despite the particular personalities involved.

I hope the Commerce Department and all of the Federal agencies of our country keep this principle in mind as they take the long overdue steps to improve the security of sensitive data when the American people have entrusted them or that they have entrusted us, rather, to protect.

When they give us their information, very often involuntarily, we have a sacred duty to protect their privacy and the integrity of that information, and we cannot look at it any less solemnly than that.

Thank you, Mr. Chairman.

[The prepared statement of Hon. W.J. "Billy" Tauzin follows:]

PREPARED STATEMENT OF HON. W.J. "BILLY" TAUZIN, CHAIRMAN, COMMITTEE ON ENERGY AND COMMERCE

Thank you, Mr. Chairman, and I want to echo your comments regarding the need for all Federal agencies to start devoting the attention and resources necessary to secure their computer systems from attacks or misuse. The government must do more to protect the sensitive personal, financial, proprietary and national security-related data on its systems.

I also want to stress how valuable the work of this Subcommittee has been in moving the ball forward on these issues. There should be little doubt in anyone's mind that, absent the aggressive oversight of this Subcommittee, agencies such as EPA, DOE, HCFA (now known as CMS) and others would not have taken many of the actions that they recently have taken to improve the security of their sensitive data and systems. While none of them are yet perfected, and none will likely ever be perfected due to rapidly changing technology, keeping the pressure and the focus on these issues is critically important to our nation and to its citizens.

As for the Commerce Department—which is the focus of our hearing today—the GAO and Inspector General audit findings are alarming. Ethical hackers from GAO and the Inspector General's office were able to have their way with the Depart-

ment's various computer systems—violating the integrity of the Department's computer networks virtually at will.

While these findings are quite troubling, they don't surprise me at all, based on the Committee's work at other agencies. When an Administration, such as the Clinton Administration, devotes so little attention and resources to a particular matter, we shouldn't be surprised to find that such problems are so pervasive. It is clear to me that, despite what the former President might have said about the importance of computer security, his Administration failed to take actions to make the protection of our nation's critical cyber assets a true priority.

That is why I am so pleased to see that the new Secretary of Commerce is taking a different approach. He's instituted a new management structure—with increased authority, responsibility, and accountability for the Department's information officers. He's allocated more resources to these security functions at the Department level. And, probably most importantly, the Secretary has made clear to his Under Secretaries that they will make computer security a priority as an integral part of their programmatic missions, and will allocate additional resources as necessary to get the job done.

In this vein, we are pleased to have the newly-confirmed Deputy Secretary of the Department here today to testify, signaling the importance of this topic to the Secretary and the level at which these issues are now being handled within the Department.

Let me finish just by emphasizing that good computer security is not a simple fix. While it takes consistent and sustained leadership, particularly in the beginning, effective long-term information security programs require the implementation of sound processes and policies that can carry on absent, or despite of, particular personalities. I hope the Commerce Department, and all Federal agencies, keep this principle in mind as they take these long-overdue steps to improve the security of the sensitive data which the American people have entrusted them to protect.

I thank the Chairman, and yield back the balance of my time.

Mr. GREENWOOD. The Chair thanks the chairman for his comments and for his presence and for his assistance and cooperation and help with this investigation, and recognizes for an opening statement the gentleman from North Carolina, Mr. Burr.

Mr. BURR. I thank the chairman and full committee chairman.

Having finished a hectic legislative schedule this week, if we look a little tired, it is because we are, and this committee contributed greatly to major legislation in the form of a comprehensive energy package and a patient's bill of rights that some dreamed would never happen.

But the issue that we are here to look at today is of interest to every member, Republican and Democrat. That is certainly not indicative of the participation that we have this morning. It is more indicative of the lack of sleep that all have had and their anxiousness to go home since the business is over.

This subcommittee has looked at computer security issues at a number of government agencies. As troubling as many of the problems that those agencies were, and still are in many cases, I am especially troubled by some of the concerns raised by the General Accounting Office audit of seven Commerce bureaus.

In particular, I am more than a little concerned about the security of the Bureau of Export Administration, which is responsible, among other things, for regulating the export of sensitive goods and technology, enforcing export controls, anti-boycott and public safety laws, cooperating with and assisting other countries on export control and strategic trade issues, assisting U.S. industry to comply with international arms control agreements, and monitoring the viability of the United States' defense industrial base.

That mission statement came straight off BXA's Web site. I imagine most of us recognize those as some very serious respon-

sibilities, and I imagine most of us will be equally disturbed by the fact that BXA has one of the worst computer security problems and is among the most susceptible to unauthorized access of the seven bureaus examined by GAO.

I suspect, based on the track record, that it is not a stand out among the rest of the department's bureaus either. Apparently BXA had not tested its system since 1991 and had not conducted a risk assessment since 1994.

Many of the problems GAO will discuss were also identified by the Commerce Inspector General in a 1999 report. Here we are today, August 2001. It must be Groundhog Day, starting at the same point with the same problems once again.

Now, what this means is that the Commerce Department has apparently not made much progress adhering to PDD 63 issued in May 1998 that set up groups within the Federal Government to develop and implement plans that would protect government operated computer and communications infrastructure.

The directive identified 12 areas critical to the functioning of this country. Commerce was designated as lead agency for information and communications security. Foreign affairs and national defense are also key elements of the directive, and it is my understanding that the export control system is considered, under PDD 63, critical.

And I have the sneaking suspicion that GAO is about to tell this subcommittee that it was able to gain unauthorized access to administrative level BXA systems.

That's not the only portion of the mission statement on the Web site. It also states that another of the bureau's missions is to promote Federal initiatives and public-private partnerships across industry sectors to protect the Nation's critical infrastructure. To protect the Nation's critical infrastructure. I think that one phrase justifies why we are here today, and I think why everybody takes it seriously.

In closing, I will say to our friends from the Department of Commerce: you inherited this problem. The challenge is that you have inherited a problem you have to fix.

I hope the next Congress with the next Commerce Department—hopefully they are the same people we have today in the next Commerce Department—but heaven forbid we ever have a situation where we come back up here to talk about this problem again because I believe that this committee is serious about making sure that we work as a partner to make sure that the problem of security within BXA, within Commerce, within all Federal agencies is eliminated as it relates to the access that we've seen.

Mr. Chairman, once again, let me thank you, and yield back the balance of my time.

Mr. GREENWOOD. The Chair thanks the gentleman for his statement and welcomes our first two witnesses.

They are the Honorable Johnnie E. Frazier, Inspector General, U.S. Department of Commerce, and Mr. Robert F. Dacey, Director of Information Security Systems at the U.S. General Accounting Office.

You gentlemen are aware that the committee is holding an investigative hearing, and when doing so has had the practice of taking

testimony under oath. Do you have any objections to testifying under oath?

Mr. FRAZIER. No, sir.

Mr. GREENWOOD. Seeing no such objections, 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 today?

Seeing a negative response, in that case if you would please rise and raise your right hands, I will swear you in.

[Witnesses sworn.]

Mr. GREENWOOD. Thank you.

You may be seated, and you are now under oath, and, Mr. Frazier, we will begin with you for your opening statement.

Please proceed. Welcome.

TESTIMONY OF HON. JOHNNIE E. FRAZIER, INSPECTOR GENERAL, U.S. DEPARTMENT OF COMMERCE; AND ROBERT F. DACEY, DIRECTOR, INFORMATION SECURITY ISSUES, U.S. GENERAL ACCOUNTING OFFICE

Mr. FRAZIER. Thank you, Mr. Chairman.

Mr. Chairman and members of the committee, I am very pleased to be here today to talk about the OIG's work as it relates to the Department of Commerce IT security.

The detailed results of our work have been included in my long statement, which I would like to have submitted for the record, but I would like to take a few minutes right now just to talk about a few of the projects that we have been working on.

Commerce, as you know, has many complex computer systems that provide essential services to the public and support critical mission activities, such as the Nation's weather services, care of the environment, promotion of trade, economic growth, and scientific research.

As the department's systems have become more interconnected, vulnerabilities have also increased, thus increasing the need to continuously improve IT security measures. I cannot overemphasize the importance of IT security.

Indeed, in our recent semi-annual reports to the Congress, we have identified strengthening department-wide security over information technology as one of the top ten management challenges facing the Department of Commerce.

During the past year, we have engaged in various audit, inspection, evaluation, and investigation activities aimed at strengthening IT security Commerce-wide. We have coordinated with GAO and the CIO to ensure that we address the most important issues and avoid duplication of effort.

In our resulting reports and briefings, we have made numerous observations and recommendations aimed at improving IT security. Let me briefly mention a few of our efforts.

One recent evaluation which examined the Office of the CIO's oversight of the department's IT security program found that despite some progress in recent years, additional improvements are needed. The department's IT security policy needs to be revised and expanded because it has not been updated to comply with sig-

nificant revisions of OMB guidance, and it has not kept pace with recent trends in technology and related security threats.

Additional IT security compliance procedures are needed because security for many of the department's systems has not been adequately planned. The security reviews have not been performed, and several of our agencies do not even have adequate awareness plans or training plans or even sufficient capabilities for responding to IT security incidents.

Another one of our evaluations revealed that although the department made early strides in its critical infrastructure protection planning, important milestones had slipped. The inventory of critical assets needed to be reevaluated and vulnerability assessments, remediation plans, and budget justifications just simply had not been completed.

A third evaluation identified privacy and security concerns raised by the department's use of Internet "cookies" and Web "bugs" on its Web sites.

We have also identified security issues through our inspections of Commerce offices and activities, both domestically and overseas. Likewise our investigative work has identified and examined specific incidents or allegations involving IT security weaknesses, vulnerabilities, or threats.

And finally, our systems security audits of departmental financial management systems are designed to identify IT security problems. These audits are performed by certified public accounting firms under contract with us and include security reviews of the department's financial management systems and related networks.

The CPAs use the GAO Federal information system controls audit manual as their guidance.

The fiscal year 2000 financial statement audits included review of general system controls at the department's seven data processing locations. We found weaknesses at all seven locations, including our observations that formal security plans either did not exist, were outdated, or were not approved for the major financial management systems and associated support systems.

Moreover risk assessments needed to be completed and approved, and more security monitoring was clearly needed.

In addition to the general system security control reviews, penetration testing was also performed at four of the seven locations to identify weaknesses in access controls. The penetration testing found open modems and ports that were accessible to potential hackers, readily accessible sensitive information on Web sites, and firewall configurations that could allow a hacker to introduce a virus.

As for physical security, some computer rooms in sensitive work areas were not adequately secured.

It is important at this point to note that the department and its operating units have reported progress on some of these weaknesses, and I should also note that we are aware that they are working to address others.

But you should also note that we are in the process of performing our annual follow-up work to try and confirm many of these observations and reported accomplishments.

We currently have other IT security reviews underway, including looking at some of the classified systems, looking at the background investigations behind some of the people who run these systems and a host of other projects.

Finally, I am pleased to note that just last month my office entered into a memorandum of agreement with the department's Office of the CIO and the Office of Security to define our respective roles and responsibilities related to Commerce's IT security program. This agreement is intended to promote a partnership among the three offices to ensure improved coverage of IT security matters.

In closing, it is clear to me that cooperative, continuous, and concerted efforts are needed by each of us, and I mean each of us, as we move to address IT security weaknesses. These same efforts are needed if we are to have any chance of at least staying one step ahead of hackers and others that see IT security as some sort of cat and mouse game.

I am encouraged that the senior management of the department and its operating units increasingly recognize the need to take a proactive approach to do this. For example, the Secretary's recent directive increasing the authority of operating unit CIOs and making them a more integral part of the bureau management team is an important initiative.

Likewise, the recent appointment of the Senior Advisor to the Secretary for Privacy should be instrumental in addressing such issues as "cookies," Web "bugs," and other security and privacy matters.

Program officials are being strongly reminded that they, too, have key IT security responsibilities and need to work closely with operating CIOs and security officials to ensure a more effective security program.

This concludes my statement, and I will gladly answer any questions.

[The prepared statement of Hon. Johnnie E. Frazier follows:]

PREPARED STATEMENT OF JOHNNIE E. FRAZIER, INSPECTOR GENERAL, U.S. DEPARTMENT OF COMMERCE

Mr. Chairman and Members of the Committee, I am pleased to appear before you today to discuss the Office of Inspector General's (OIG) work and other activities related to the security and protection of the Department's critical information technology (IT) systems, programs, and activities.

The Department of Commerce has numerous complex computer systems that provide essential services to the public and support critical mission activities, such as the nation's weather services, environmental stewardship, promotion of trade and economic growth, scientific research, and technological development. As the Department's systems have become more interconnected, vulnerabilities have also increased, thus increasing the need to continuously improve IT security measures. Strong IT security measures are vital to (1) protecting the privacy of information, (2) safeguarding the integrity of computer systems and their networks, and (3) ensuring the availability of services to the American public and other users. I cannot emphasize too much how important these measures are.

Indeed, in our recent *Semiannual Reports to the Congress,* we have identified "Strengthening Department-wide Information Security" as one of the top 10 management challenges facing the Department of Commerce because of that issue's:

1. Importance to the Department's mission and the nation's well-being,
2. Complexity and sizable expenditures, and
3. Need for significant management improvements.

During the past year, we have engaged in a number of audit, inspection, evaluation, and other activities involving Commerce IT security matters—all aimed at strengthening IT security Commerce-wide. We have completed evaluations of the Department's efforts to implement its Critical Infrastructure Protection (CIP) plans. We also have assessed the Office of the Chief Information Officer's (CIO) IT security policy and the effectiveness of its oversight of the Department's IT security program. In addition, we have evaluated the use of persistent Internet "cookies" and "web bugs" on Commerce Internet sites. Furthermore, in support of the OIG's fiscal year 2000 financial statement audits, we have conducted security reviews of the Department's financial management systems and their related networks.

Moreover, assessments of IT security policies and practices are often an integral part of the operational inspections we conduct of Commerce activities, units, and offices domestically and overseas. These inspections are intended to provide operating unit managers with useful, timely information about their operations, including IT security issues. IT security problems have also been identified through our investigative work. In addition, we have worked closely with many of the Department's key IT managers, top security personnel, and senior program officials in an effort to identify the most critical IT security issues and help craft corrective measures. Let me briefly summarize the results of some of our recent efforts.

EARLY PROGRESS MADE IN CRITICAL INFRASTRUCTURE PROTECTION, BUT PLANNING AND IMPLEMENTATION HAVE SLOWED

Last year, we evaluated the Department's CIP plan, identification of minimum essential infrastructure (MEI) assets, and vulnerability assessments of its cyber-based assets. MEI assets are the physical and cyber-based assets essential to the minimum operations of the economy and the government. Our evaluation found that although the Department had made initial progress by developing a Department-wide CIP plan, identifying critical infrastructure assets, and initiating vulnerability assessments, there were several areas that warranted management attention:

- The Department's CIP plan needed to be strengthened because several of its elements were outdated or missing, and important milestones had slipped. The asset inventory, vulnerability assessment framework, and budget estimates included in the plan were not current. The plan also did not include requirements for reviewing new assets to determine whether they should be included as MEI assets, periodically updating vulnerability assessments, or developing a system for responding to infrastructure attacks.
- The MEI asset inventory needed to be reevaluated because of limitations in data gathering. In most cases, asset managers were neither interviewed nor given adequate guidance before filling out complex questionnaires used to gather asset information, and the officials most knowledgeable about the assets were seldom interviewed because of logistical problems and limited resources. Establishing a reliable MEI inventory is important because it forms the basis for later activities, such as selecting the highest risk assets for vulnerability assessments and taking remedial actions.
- Vulnerability assessments, remediation plans, and budget justifications needed to be completed. Reportedly due to resource constraints, the Department had current vulnerability assessments for less than 10 percent of MEI assets and had not developed any remediation plans.

The CIO's office agreed with our findings and stated that the Department's focus would be on the broad spectrum of IT security, which emphasizes assets critical to the Department's mission and includes most cyber-based MEI assets. Short-term actions were identified to improve guidance to operating unit personnel involved in vulnerability assessments and increase their involvement in the MEI asset inventory, revise the MEI asset list, and evaluate new assets to determine whether they should be included as MEI assets.

ADDITIONAL FOCUS NEEDED ON IT SECURITY POLICY AND OVERSIGHT

The CIO is responsible for developing and implementing a departmental IT security program to ensure the confidentiality, integrity, and availability of information and IT resources. The CIO's responsibilities include developing policies, procedures, and directives for IT security and providing oversight of the IT security programs of the Department's operating units.

We conducted an evaluation to assess the CIO's policies and the effectiveness of his oversight of the Department's IT security program. Our review focused on the CIO's compliance with laws and regulations governing IT security and his actions in recent years to oversee the Department's IT security program.

We found that although in the past IT security did not receive adequate attention, in more recent years, the CIO's office had expanded its focus on and increased the resources devoted to IT security. For example, the office conducted its first Department-wide assessment of IT security planning in 1999 and reviewed operating unit self-assessments in 2000, which resulted in increased compliance with security requirements. Nevertheless, policy and oversight need further improvements. Specifically:

- **IT security policy needs to be revised and expanded.** The Department's IT security policy is out of date because it was developed in 1993 and 1995, prior to a significant revision of OMB Circular A-130, which communicates policy on the security of federal automated information resources. The policy is also missing important components because it has not kept pace with recent trends in technology and related security threats. The Department's policy must be kept current and complete because the operating units use it as the foundation for their general and system-specific policies. We recommended that the CIO's office update and expand its IT security policy as soon as possible.
- **Additional IT security compliance procedures are needed.** Security for many of the Department's systems has not been adequately planned, and security reviews have not been performed. In addition, several operating units do not have adequate awareness and training programs or adequate capabilities for responding to IT security incidents. The Government Information Security Reform Act (GISRA) requires the CIO's office to conduct annual IT security evaluations in 2001 and 2002 similar to the self-assessments it monitored in 2000. We recommended that the office commit to a program of reviews that extends beyond GISRA's 2-year review requirement. Moreover, the CIO's office should work with the Department's acquisition and budget managers to ensure that IT-related procurement specifications include security requirements, and that funds for meeting these requirements are included in operating unit budgets.

During our evaluation of the Department's IT security policy, we provided the Department with a written analysis that identified weaknesses and deficiencies in the policy, and made recommendations for specific changes to bring the policy into compliance with applicable laws and regulations.

The CIO's office agreed with all of our recommendations and cited a number of corrective actions it planned to take to implement them. Among other things, it agreed to revise, expand, and update the Department's IT security policy; continue its compliance review program beyond the 2-year period required by GISRA; and begin security reviews as soon as possible.

USE OF INTERNET "COOKIES" AND "WEB BUGS" RAISED PRIVACY AND SECURITY CONCERNS

We evaluated the use of persistent Internet cookies and web bugs by departmental Internet sites, as well as the adequacy of the privacy statements posted on the main web pages of the Department and its operating units. We conducted our evaluation in response to Public Law 106-554, the Consolidated Appropriations Act of 2001, which required the Inspector General of each agency to submit a report to the Congress disclosing any activity regarding the collection of information relating to any individual's access or viewing habits on the agency's Internet sites.

Persistent Internet cookies are data stored on web users' hard drives that can identify users' computers and track their browsing habits. Web bugs are software code that can monitor who is reading a web page. These technologies are capable of being employed in ways that could violate the privacy of individuals visiting the Department's web sites and can also pose security threats.

Web bugs are considered security threats because they can perform malicious actions, including searching for the existence of specific information, such as financial information, on a user's hard drive, and downloading files from, or uploading files to, a user's computer. A web user would be unaware of the presence of web bugs without using detection software. Even if such software were used, the malicious actions performed by identified web bugs could go undetected.

We found that most of the Department's Internet sites do not use either persistent cookies or web bugs. However, we did find several instances in which persistent cookies were being used without a compelling reason or the approval of the Secretary, as required by Department and OMB policy. We also found a number of web pages using web bugs. At the time we began our evaluation, the Department did not have a policy regulating web bug use, but it promptly developed and issued one when informed of the problem. Finally, we found that many of the operating units'

privacy statements did not provide all of the information required by the Department's privacy policy.

We recommended that the Department's CIO direct operating unit CIOs and senior management to implement a strategy to control the use of persistent cookies and web bugs and to certify annually that the operating unit is in compliance with the Department's applicable policies. We also recommended that the CIO direct operating unit CIOs and senior managers to revise their privacy policy statements to make them compliant with the Department's policy. The CIO's office agreed with our findings and worked with us to help ensure that the cookies we had identified were removed. The Secretary of Commerce's new Special Assistant for Privacy is working to remove all web bugs and develop a uniform privacy policy statement.

SYSTEMS SECURITY AUDITS OF DEPARTMENTAL FINANCIAL MANAGEMENT SYSTEMS REVEAL PROBLEMS

Our audits of Commerce operating units' financial statements, performed by certified public accounting (CPA) firms under contract with us, include security reviews of the Department's financial management systems and related networks that support the statements. Our CPA contractors use GAO's *Federal Information System Controls Audit Manual* (FISCAM) as a guide in performing these reviews. FISCAM provides guidance on assessing the reliability of computer-generated data that supports financial statements, including physical security and logical access controls designed to prevent or detect unauthorized access or intrusion into systems and networks.

In 1999 we adopted a systems security review strategy that provides for full coverage of each financial management system and its related networks on a two-year basis. Every two years, a review addresses the six systems security areas identified in FISCAM: (1) *entitywide security program planning and management,* (2) *access controls,* (3) *application software development and change control,* (4) *systems software,* (5) *segregation of duties,* and (6) *service continuity.* In the alternate years, we routinely conduct penetration testing (in which someone playing the role of a hostile attacker tries to compromise systems security) and application-level testing. Review of the system environment for significant changes and follow-up on open recommendations occurs annually.

The audits of operating units' individual fiscal year 2000 financial statements included reviews of the general system controls over the major financial management systems at the seven data processing locations. In the reports on our audits of the Department's fiscal year 1999 and 2000 consolidated financial statements, we noted that these systems security reviews disclosed weaknesses in controls over major financial management systems at all seven locations that provide data processing support. Specifically, these reviews found that:

1. *Entitywide security program planning and management* needed improvement at all seven locations. This control is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. It is intended to ensure that security controls are adequate, consistently applied, and monitored, and that responsibilities are clear and properly implemented.
2. *Access controls* for both operating systems and the financial management systems needed strengthening at all seven locations, and monitoring of external and internal access to systems needed strengthening at five locations. These controls should limit or monitor access to computer resources to guard against unauthorized modification, loss, and disclosure.
3. *Applications software development and change control* needed improvement at four locations. These controls should help prevent the implementation of unauthorized programs or modifications to existing programs.
4. *Systems software* improvements were needed at four locations. Controls in this area should limit and monitor access to the important software programs that operate computer hardware.
5. *Segregation of duties* improvements were needed at five locations. Appropriate controls in this area include policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets.
6. To ensure *service continuity,* contingency plans needed to be prepared, updated, or improved at all seven locations. Appropriate controls in this area include procedures for continuing critical operations, without interruption and with prompt resumption of those operations, when unexpected events occur.

Of particular note, among the weaknesses identified by the CPA firms in the area of entitywide security program planning and management, was the fact that formal

comprehensive security plans either did not exist, were outdated, or were not approved for the major financial management systems and associated general support systems on which the applications were processed. In addition, risk assessments needed to be completed and approved, and security monitoring needed to be performed.

At four locations, penetration testing was also performed on the network that supports the financial management systems to identify weaknesses in access controls. As part of the penetration testing, the CPA firms reviewed the adequacy of access controls, which include logical and physical controls. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access, such as by hackers, to networks, systems, and sensitive files by requiring users to input user ID numbers, passwords, and other identifiers that are linked to predetermined access privileges. Physical controls involve keeping computers in locked rooms to limit physical access. The firms' penetration testing of logical controls found that in some cases:

- Open modems and ports were accessible to potential hackers.
- Sensitive information on websites was readily accessible.
- Sensitive active system services could allow unauthorized access, downloading of files, and gathering of information.
- Firewall configurations could allow a hacker to introduce a destructive virus.

In addition, physical access controls over networks and financial management systems needed strengthening. For example, at one location, automated exterior locking systems had not been installed on doors to restrict access, and the key card lock for the data center's computer room was inappropriately placed on the inside of the door, rather than the outside. In addition, personnel did not consistently lock and secure their work areas. At another location, hardware that processed very sensitive information was located in an area accessible by numerous employees and contractors and was not segregated in an individually secure area.

For fiscal year 2000, the CPA firms concluded that four operating units had system security weaknesses that rose to the level of "reportable conditions." Taken together, these conditions, combined with the Department's lack of an integrated financial management system, constituted a material weakness in the audit of the consolidated financial statements. In our report on the audit of the consolidated statements, we recommended that the CIO's office continue to develop and implement a database for tracking and reporting on corrective actions planned and taken to address the outstanding general controls recommendations. We also recommended that the office review, monitor, and provide guidance to the reporting entities on their corrective actions planned and taken in response to our current and prior years' audit reports on general controls.

We issued audit reports with recommendations to correct the control weaknesses identified at each of the seven data processing locations, and the operating units generally agreed with our recommendations. The Department and its operating units are required to provide us with audit action plans that address each of our recommendations. We have reviewed the plans submitted to date and concur with the actions taken or planned. Moreover, we are in the process of performing our annual follow-up of the adequacy of the corrective actions planned or taken.

IT SECURITY ISSUES HAVE ALSO BEEN IDENTIFIED THROUGH OIG INSPECTIONS AND INVESTIGATIONS

We have also identified IT security issues through our inspections and investigative work. Our inspections unit, for example, conducted a 1999 assessment of the Bureau of Export Administration's (BXA) Export Control Automated Support System as part of a larger review of BXA's administration of the federal export licensing process for dual-use commodities. While we determined that most of the system's general and application controls were adequate, we found that BXA's IT security controls could be enhanced by improving database access controls, preparing a security plan, performing periodic security reviews, officially assigning the security duties to its security officer, providing all users with current security training, and restricting the number of BXA employees with file manager access. BXA management implemented some corrective actions immediately and agreed to take action on our other recommendations dealing with the IT security of its licensing system.

We are also conducting a series of inspections of the National Weather Service's weather forecast offices (WFOs) that have identified a number of IT security issues that need to be addressed by local managers. Among other problems, we noted that one WFO we visited did not have a designated security officer, and office personnel did not follow the Weather Service's policy on IT security. We found other problems, which I cannot describe in detail in a public hearing, that highlight how vulnerable

some systems can be without proper management attention. Fortunately, the Weather Service has greatly improved its IT security both locally and nationally since the start of our review. During the past nine months, we visited two other WFOs. Although we continued to identify some IT security problems, we have found that designated security officers have been named and are receiving necessary training on IT security. More importantly, WFO personnel appear to better understand IT security concepts and requirements.

IT security problems have also been identified through our investigative work. Through our OIG Hotline and other information channels, specific incidents or allegations involving IT security weaknesses, vulnerabilities, or threats have been brought to our attention and examined. For example:

- In one incident, a foreign hacker penetrated a network server and installed software without the knowledge of the system administrator. Had the software been activated, the server would have been prevented from performing its normal network services and would have been one of many computers simultaneously activated to overload a designated Internet site. As a result of the incident, the number of points of access to the network was reduced to a bare minimum, and existing monitoring software was activated.
- In another incident, a hacker caused extensive damage to an operating unit server, and it took more than 5 work days to repair the server and restore operations. Because the software on the server was destroyed, the system administrator was not able to determine how the attack had occurred. Security features were added when the software was restored, to reduce the risk of another shutdown.
- In a third incident, an after-hours contract cleaning employee used a computer that had not been properly secured to gain access to the Internet via a network system and view pornographic materials. Coordination with the contracting officer, property manager, and president of the contract company resulted in the employee's immediate removal from the facility contract and subsequent termination. In addition, the practice of routinely leaving the computer on overnight was discontinued.

ADDITIONAL OIG REVIEWS OF IT SECURITY MATTERS ARE EITHER UNDERWAY OR PLANNED

We are currently conducting IT security evaluations related to (1) the Economics and Statistics Administration's and the Census Bureau's preparation and release of the Advance Retail Sales Principal Economic Indicator, (2) the Department's classified information systems, and (3) the Department's IT security program and practices, as required by the Government Information Security Reform Act.

The objective of our security evaluation of the Advance Retail Sales indicator is to determine whether adequate internal controls and system safeguards are in place to prevent the unauthorized disclosure or use of the economic indicator data before its release to the public. We have found that employees dealing with the indicator do not always have appropriate background investigations and that their positions are not always assigned the appropriate level of risk as required by Title 5, Part 731, of the Code of Federal Regulations and OMB Circular A-130. In some instances, the Department's records did not identify the type of investigation done, if any, for personnel working on Principal Economic Indicators. We also noted a lack of guidance from the Office of Human Resources Management, as well as from the Office of Security, suggesting that the problems associated with assigning appropriate risk levels to positions and ensuring that background investigations are performed may exist throughout Commerce. We are conducting additional work to examine this issue.

Our review of the Department's classified information systems will assess the adequacy of its policies for protecting classified information and the effectiveness of its oversight of these systems.

The GISRA-mandated review is the annual evaluation of the Department's IT security program and practices. This evaluation will incorporate information from our security reviews, as well as results of related evaluations performed by operating units, GAO, and contractors. We are also continuing our security reviews of Commerce's financial management systems and related networks as part of our fiscal year 2001 financial statements audits. These reviews will be in line with our IT security review strategy and will include penetration testing of the U.S. Patent and Trademark Office and FISCAM reviews for the other operating units.

The need for the OIG to provide oversight and evaluation of IT security will be increasingly critical in the coming years. Our independent evaluation of the Department's IT security program being performed under GISRA and our security reviews

of the Department's financial management systems show that although the Department is giving greater attention to IT security, serious issues remain to be resolved. These issues appear to be the result of an earlier lack of attention to IT security, limited resources, and an environment in which the risks, threats, and vulnerabilities have continued to escalate in number and complexity. The weaknesses identified by GAO's recent network vulnerability analysis of the Department underscore our concerns.

In our independent GISRA evaluation for the next fiscal year, we plan to evaluate the effectiveness of operating unit IT security programs and to conduct security evaluations of specific general support systems and major applications. We will use the findings of our current GISRA evaluation and of GAO's security audit to assist us in identifying specific operating units, general support systems, and major applications to evaluate in the future.

COOPERATIVE EFFORTS NEEDED TO ADDRESS IT SECURITY WEAKNESSES

I am pleased to note that, just last month, my office entered into a memorandum of agreement with the Department's Office of the CIO and Office of Security to define our respective roles and responsibilities relating to the development, implementation, and management of the Commerce IT security program. This agreement is intended to promote a partnership among the three offices that both ensures complete coverage of IT security matters and prevents wasteful duplication of effort.

Under the agreement, the CIO's office has the basic responsibility for developing and implementing the Commerce-wide IT security program, which includes developing IT security policies and procedures, promoting IT security awareness and training, serving as the Department's critical infrastructure assurance officer, and convening a meeting of the incident response group when incidents or intrusions occur. Commerce's Office of Security has the primary responsibility for security for the Department's classified systems and, in conjunction with the Department of State, for IT security at Commerce overseas posts. My office is responsible for conducting investigations of IT incidents and intrusions, and for conducting reviews of the Department's IT security program and individual systems, including the annual independent evaluations of the program required by GISRA.

In closing, it is clear that cooperative, continuous, and concerted efforts are needed by each of us—and I mean each of us—if we are to address IT security weaknesses. These efforts are needed if we are to have any chance of staying at least one step ahead of the hackers and others that see IT security as some sort of cat-and-mouse game.

I am confident that the senior management of the Department and its operating units increasingly recognize the need to take a proactive approach to do this. For example, the Secretary's recent directive increasing the authority of operating unit CIOs and making them a more integral part of the management team is an important initiative. Likewise, the recent appointment of a Senior Advisor to the Secretary for Privacy should be instrumental in addressing such issues as cookies, web bugs, and other security/privacy matters. And program officials are also being strongly reminded that they too have key IT security responsibilities and need to work closely with operating unit CIOs and security officials to ensure an effective security program.

We intend to continue our partnership with all of these managers by identifying weaknesses and potential vulnerabilities in IT security and by searching for ways to improve it. Through this relationship, I believe we can help strengthen IT security within the Department.

This concludes my statement. A list highlighting some of the reports we have issued that address IT security issues is included as an attachment. Mr. Chairman, I would be happy to answer any questions you or other members of the Committee might have.

ATTACHMENT

U.S. DEPARTMENT OF COMMERCE

OFFICE OF INSPECTOR GENERAL

RECENT AUDIT, INSPECTION, AND EVALUATION REPORTS ON INFORMATION TECHNOLOGY SECURITY MATTERS

Evaluations

1—Office of the Chief Information Officer: *Use of Internet "Cookies" and "Web Bugs" on Commerce Web Sites Raises Privacy and Security Concerns,* OSE-14257, April 2001

2—Office of the Chief Information Officer: *Additional Focus Needed on Information Technology Security Policy and Oversight,* OSE-13573, March 2001

3—Office of the Chief Information Officer: *Critical Infrastructure Protection: Early Strides Were Made, but Planning and Implementation Have Slowed,* OSE-12680, August 2000

4—Bureau of the Census: *Computer Security for Transmission of Sensitive Data Should Be Strengthened,* OSE-10773, September 1998

Financial Statements Audits

[Note: These audits are performed annually; listed below are only the reports covering FY 2000. In addition, the reports on security reviews are not publicly available documents.]

5—Department of Commerce: *Consolidated Financial Statements, FY 2000,* FSD-12849-1, March 2001

6—National Institute of Standards and Technology, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12859-1, February 2001

7—Economic Development Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12851-1, January 2001

8—Bureau of the Census, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12850-1, January 2001

9—National Technical Information Service, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12857-1, January 2001

10—Office of the Secretary, *Follow-up Review of the General Controls Associated with the Office of Computer Services/Financial Accounting and Reporting System,* FSD-12852-1, January 2001

11—International Trade Administration, *Review of General and Application System Controls Associated with the Fiscal Year 2000 Financial Statements,* FSD-12854-1, January 2001

12—National Oceanic and Atmospheric Administration, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12855-1, December 2000

13—United States Patent and Trademark Office, *Improvements Needed in the General Controls Associated with Financial Management Systems,* FSD-12858-1, December 2000

Inspections

14—National Oceanic and Atmospheric Administration: *San Angelo Weather Forecast Office Performs Its Core Responsibilities Well, but Office Management and Regional Oversight Need Improvement,* IPE-13531, June 2001

15—National Oceanic and Atmospheric Administration: *Raleigh Weather Forecast Office Provides Valuable Services, but Needs Improved Management and Internal Controls,* IPE-12661, September 2000

16—Bureau of Export Administration: *Improvements Are Needed to Meet the Export Licensing Requirements of the 21st Century,* IPE-11488, June 1999

17—Office of Security: *Vulnerabilities in the Department's Classified Tracking System Need to Be Corrected,* IPE-11630, March 1999

Mr. GREENWOOD. We thank you very much for your testimony, and we will be getting to questions shortly.

Mr. Dacey.

TESTIMONY OF ROBERT F. DACEY

Mr. DACEY. Mr. Chairman and members of the committee, I am pleased to be here today to discuss our review of information security controls over unclassified systems at the Department of Commerce.

As you requested, I will briefly summarize our written testimony.

At the seven Commerce operating units we reviewed, significant and pervasive computer security weaknesses place sensitive Commerce systems at serious risk. We demonstrated through commonly or readily available software and common techniques that individuals, both internal and external to Commerce, could gain unauthorized access to these systems and thereby read, copy, modify or delete sensitive financial, economic, personnel and confidential business data.

Moreover, intruders could disrupt the operations of mission critical systems, and due to poor incident detection capabilities, unauthorized system access may not be detected.

As an illustration of these points, a recent media report announced the discovery of security vulnerabilities that allowed sensitive business information to be publicly accessed from a Commerce Web site, forcing the department to temporarily shut down a part of that site.

Our review identified vulnerabilities in four key areas. First, controls intended to protect information systems and critical data from unauthorized access were ineffectively implemented, leaving systems highly susceptible to intrusions or disruptions.

Specifically, management of user IDs and passwords, including those related to powerful system administration functions, were not effective. As you alluded to earlier, in many systems passwords were not required or were easy to guess.

Also, bureau operating systems were not securely configured, including exposing excessive amounts of system information and allowing unnecessary or poorly configured system functions to exist.

Further, none of the Commerce bureaus reviewed had effective external and internal network security controls. Our testing demonstrated that extensive unauthorized access to the department's networks and systems could be gained as a result of weakly configured external control devices, poorly controlled dial-up modems, and ineffective internal network controls.

Second, we found other significant weaknesses. Specifically, computer duties were not properly segregated to mitigate the risk of errors and fraud.

Software changes were not adequately controlled to ensure that only authorized and tested programs were put in operation, and comprehensive and complete recovery plans were not developed to ensure the continuity of operations in the event of a service disruption.

Third, Commerce bureaus did not adequately prevent, detect, respond to, or report intrusions, providing little assurance that unauthorized attempts to gain access to its systems would be identified and appropriate actions taken in time to prevent or mitigate damage.

For example, software updates to correct known vulnerabilities were not installed, tested bureaus were generally unable to detect our extensive intrusion activities, and in two instances when our activity was detected, Commerce employees inappropriately responded by launching attacks back against our systems.

Moreover, these two incidents were not reported to the security managers of the various bureaus.

Also, we identified evidence of hacker activity that Commerce had not previously detected on a system containing sensitive personnel information.

Fourth, and most important, Commerce does not have an effective, department-wide information security program, as Mr. Frazier earlier discussed, to proactively insure that sensitive data and critical operations are adequately protected.

The lack of an effective security program is exacerbated by the highly interconnected nature of Commerce's systems. Key weaknesses existed in each of five critical areas.

First, there was lack of a strong, centralized management function to oversee and coordinate department-wide security activities.

Second, there was a widespread lack of risk assessment. For example, as of March 2001, of the bureau's 94 sensitive systems we reviewed, 91 did not have documented risk assessments, 87 had no current security plans; and none were authorized for processing by Commerce management.

Third, there were significantly outdated and incomplete information security policies which did not reflect current Federal requirements in many important areas, had not been updated to reflect certain risks related to the Internet, and did not establish baseline security requirements for all systems.

Fourth, there was inadequately promoted security awareness and training. Although each of the bureaus had informal programs in place, none had documented computer security training procedures that meet Federal requirements to ensure that security risks and responsibilities are understood by all managers, users, and system administrators.

Fifth, there was a lack of an ongoing program to test and evaluate security controls. No oversight reviews of the bureau's systems had been performed by either the staff of Commerce's information security program or six of the seven bureaus. There had been isolated tests at one bureau.

In a draft report to Commerce, we made recommendations, which are summarized in our written statement, to address these weaknesses. The Commerce Secretary's response stated that Commerce has developed and is currently implementing an action plan to correct the specific problems we identified.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions that you or members of the committee may have.

[The prepared statement of Robert F. Dacey appears at the end of the hearing.]

Mr. GREENWOOD. I thank you, Mr. Dacey.

And the full statements of both witnesses will be entered into the record.

Here is a question that I would like you each to respond to. Both of you used the term "sensitive" to describe the types of systems and the data at issue here. Can you be more specific with respect to the types of information that are susceptible to compromise and why it is that Congress and the American people should be concerned about these vulnerabilities?

Mr. FRAZIER. I will be happy speak first.

There are so many systems in the Department of Commerce that we view as sensitive. You can start with the Census Bureau, for example. The Census Bureau has lots of information that is protected by Title 13, and in fact, I have heard you speak to the concern about how the American public must come to trust and know that information that they share with us is going to be protected.

Mr. GREENWOOD. That was a huge issue in this whole last census exercise where so many Americans were reluctant to fill out long forms because of the fear of compromise in the integrity of the system.

And, of course, we all assured them that that was not a problem.

Mr. FRAZIER. Yes. I should tell you that in 1998, in advance of the decennial census, we found an incredible vulnerability there, and we brought it to the attention of census managers, and that was handled as a red cover report for obvious reasons.

The concern was that if that information got out, people would begin to question whether it was wise to send in information. It was just an oversight on the part of a security manager that we could not believe, something that we would think would be as obvious as this. I am not giving the details here for obvious reasons, but we were just amazed that something as basic as that could have that kind of potential consequence to the integrity of the system.

Mr. GREENWOOD. To interrupt you for a moment, is it conceivable that a hacker could go in through the Census Bureau to my Greenwood family long forms, Census form, and scan it and identify information as being responses that our family gave to the Census form?

Mr. FRAZIER. No. When we found this problem, fortunately it was before the decennial census. It was in doing the work we did for the dress rehearsal, and so we were able to plug that gap. Of course, once you brought that to the attention of the Department and Census officials, that was something that they were going to correct immediately. So that was not a problem there.

But, again, I go back to tell you how something as important as that system would have been overlooked. You know, that was incomprehensible to us that that could be the case.

As we have gone in to look at the work at BXA, as you are aware, we have done quite a bit of work in BXA, and for many years, too many years, we have raised concerns about the adequacy of its ECASS system, which has the sensitive information on export controls, licensing requests.

We have made recommendations——

Mr. GREENWOOD. Could you elaborate on why that is sensitive? What makes that particular information sensitive?

Mr. FRAZIER. Well, part of it is business proprietary from the standpoint if you are Company X and are getting ready to export

radars to a certain country, you have to provide the department with certain information that they can use to assess your license request.

In the process of doing that, that is information that you surely do not want your competitors to have. So that would be extremely sensitive.

Mr. GREENWOOD. You mentioned radar. I assume that could apply to other military equipment that is being exported, information that we would certainly not want some individuals or organizations to have ready access to, who might have an interest in intercepting that military equipment.

Mr. FRAZIER. As you know, Commerce handles what we call dual use items, which have both military and civilian uses, and so you are right on the money when you suggest that that is information that we would surely want to protect as much as we possibly can.

Mr. GREENWOOD. In fact, in the GAO report, it says sensitive data such as relating to national security, nuclear proliferation, missile technology, and chemical and biological warfare reside in the bureau system.

Mr. FRAZIER. Yes.

Mr. GREENWOOD. Mr. Dacey, would you like to elaborate on the same subject?

Mr. DACEY. Yes. Basically, in addition to the export license information we talked about, there is certain other information. There is something called the safe harbor, which I alluded to in my oral statement, which is a method for filing to satisfy European Union privacy requirements, and by filing you demonstrate that you meet certain requirements and then can obtain certain personnel information and bring it back to your company.

And that included information like revenue, you know, what companies are you doing business with, number of employees and such nature of information which was exposed as well.

There is, additionally, other information that the bureaus have on the personal side, and that would have to do with credit card information, for example the ESA subscription services. They collect credit card information.

The bureau itself has data bases containing significant information on Commerce personnel, including various information, Social Security numbers, and that sort of thing.

So there is a variety of information, including financial information, that is out there on the systems that are at Commerce.

Mr. GREENWOOD. And what about the ability to go through the Commerce Department systems? Is it conceivable that one could go through the Commerce Department's system and then thereby reach out to consulates, to our consulates around the world?

Mr. DACEY. One of the tests that we performed, we were able to—let me back up a minute.

When we do our testing, our target or goal is to gain what we call administrative control of the systems we are looking at, and that means we could place ourselves in the position of system administrator and thereby do just about anything that we would want to do on that system, including reading files, copying files, deleting files, changing software, any number of things that a system administrator could do.

We gained that level of access on several of Commerce's systems. Some of those allowed us to gain access to networks which went to the Foreign Commercial Service posts as well as the systems that contained some of this sensitive information.

Mr. GREENWOOD. And those consulates are, of course, in turn, interconnected to other sensitive agencies of the Federal Government so that it would seem to me to heighten the sensitive nature of this leak.

Mr. DACEY. We did not specifically look at the connectivity of those Commerce installations in foreign posts with other potential agencies, but that is an issue which might be explored in the future as another task.

Mr. BURR. Would the chairman yield?

Mr. GREENWOOD. Certainly.

Mr. BURR. What I understand your answer to be that you did not try to go outside of the Commerce system within the embassy?

Mr. DACEY. That is correct. We went to Commerce installations in the various foreign posts, and because that was the limit of our testing, we stopped at that point. We did not try.

Mr. BURR. If the focus at the embassies was to keep people out of their system, but not to limit their movement from within their system that they were in, had you tried you might have been able to go anywhere within the embassy system.

Mr. DACEY. It is hard to speculate where we could have gone, but if there was interconnectivity, we had significant rights on the system, Commerce's system. We just do not know what interconnectivity might exist.

Mr. GREENWOOD. The Chair's time has expired, and the chairman recognizes the chairman of the full committee for 5 minutes to inquire.

Chairman TAUZIN. Thank you, Mr. Chairman.

Mr. Dacey, I want to understand the concept of the weakness within the system, if you do not mind. In your testimony you state that the individuals both within and outside Commerce could compromise internal and external security controls to gain extensive unauthorized access.

I want to know what you mean by "extensive." Is that another term for what is call root access or total control of the systems?

Mr. DACEY. Right. That is what I was referring to as administrative level access on the networks. That is referred to as root access, and we were able to gain that level of access on several systems.

Chairman TAUZIN. Now, you also state that the department was able to detect your extensive intrusion activities on only four occasions. How many intrusions should have been detected if they had had a good system in place?

Mr. DACEY. We attempted to scan over 1,000 system devices. So I do not say that they would detect all 1,000, but certainly we would have expected a significantly higher number of those attempts to be detected.

Chairman TAUZIN. So you are saying 4 out of 1,000 were detected?

Mr. DACEY. Over 1,000.

Chairman TAUZIN. Over 1,000?

Mr. DACEY. Yes.

Chairman TAUZIN. What is that .4 of 1 percent, something like that were detected? So that in effect, if again my math is right, something like 99.6 percent of the intrusions were not detected.

Mr. DACEY. Something like that, yes.

Chairman TAUZIN. That is purer than Ivory Snow. That is a huge number. It basically says that you could walk around undetected in cyberspace, in effect, within the department's data banks.

Mr. DACEY. Right. That is one of our concerns, as I said in my oral statement. There was actual hacker activity on one of the systems which we discovered, which Commerce was not previously aware of.

Chairman TAUZIN. Can you give me a little more information about the fact that your auditors discovered the intrusion of a Russian hacker in the system? What exactly happened there? What was going on?

Mr. DACEY. We identified a server, a network server, and when we went in to start to explore it, we identified certain tools that were left behind by a hacker, and at that point in time we turned that over to the agency and suggested that they investigate the situation and resolve it and figure out what happened.

Chairman TAUZIN. Well, did they find out what the Russian was up to?

Mr. DACEY. I believe, based on my recollection, the IG really followed up on the process afterward. I don't know if Mr. Frazier has any further information.

Chairman TAUZIN. Could you tell us?

Mr. FRAZIER. Vladimir was his name.

Chairman TAUZIN. Vladimir?

Mr. FRAZIER. Yes.

Chairman TAUZIN. Good, old Vladimir. What was Vladimir doing in our data banks?

Mr. FRAZIER. We found out that he had hacked into a number of government systems.

Chairman TAUZIN. Was he just having fun or was he up to mischief?

Mr. FRAZIER. Well, we could not determine that. He got into the system. He got into the systems at other agencies, and he did not do any major damage to our knowledge, but that is part of the problem. You do not know how long he had been there. You do not know what else he had——

Chairman TAUZIN. Well, I mean, you detected only .4 of 1 percent. So he could have been all over the place, and if he did not drop a tool here or there, you may never know he was there.

Mr. FRAZIER. We would have never known he had been there.

Chairman TAUZIN. So he could have been in a lot of other places that he did not leave his tracks, right?

Mr. FRAZIER. Yes. So what they will do is close that door.

Chairman TAUZIN. That is right.

Mr. FRAZIER. But many other doors are left open.

Chairman TAUZIN. Yes, let's talk about doors. One of the thing you mentioned, Mr. Dacey, is the interconnectivity of the Commerce Department, the bureaus you reviewed. Interconnectivity is good, of course, in a sense because it allows all of the bureaus to share information and to relate to one another. It could be a prob-

lem if a hacker or Vladimir finds, excuse my expression, the weakest link in the system and through interconnection, he is everywhere, and then bye-bye, he is gone.

Tell me about interconnectivity within the bureau, within the department, rather, among its bureaus.

Mr. DACEY. One of the issues is the interconnectivity between us. As you suggested, it is a good thing. It is used to communicate between the bureaus at Commerce. One of the issues though is protecting those systems and that interconnectivity so that if someone gains unauthorized access to one bureau system, that there are measures to prevent them from going further once they are inside the network.

What we found, in fact, was that some of the accesses that we obtained to some of the more sensitive information were actually through other bureaus that we——

Chairman TAUZIN. So you actually did that. You found the weakest link, and then bingo, you had access to other information that you might not have directly been able to access, right?

Mr. DACEY. That is correct. When we identified these, again, our tests were not designed also to detect every vulnerability, but we found sufficient evidence to——

Chairman TAUZIN. Well, I guess here is probably the most important question. Have you done enough testing to be able to advise the Commerce Department on how to seal those doors and how to protect against the Vladimirs of the world?

Mr. DACEY. We provided detailed out-briefings at the time that we performed our work in the field, and our understanding is that the agency has fixed some and is working on others, and that is consistent with their response to——

Chairman TAUZIN. Was your testing complete?

Mr. DACEY. But that was what I was going to suggest, is that we do a limited amount of testing. We spent about, let's say on average, 2 weeks at each bureau, and we found sufficient vulnerabilities to support our conclusions. I would not aver that, in fact, we found all of the vulnerabilities.

In fact, we did not find all of the vulnerabilities. One of the important steps that Commerce needs to take is really to develop an active testing program of their own and identify these vulnerabilities from a management viewpoint and fix them.

We certainly did not find them all.

Chairman TAUZIN. Mr. Chairman, one final thought, and I do not want to at all cast aspersions on either one of your operations because you do a very good job for us, but we heard from a lot of agencies that we are losing talented people, and they are reaching retirement age, and I assume that is true of your agency as well, that you are losing some of your best people.

What we have learned in this area of the high tech commerce world is that some extraordinarily good people are the youngest people, and I just wonder, are you satisfied that within your ranks are, indeed, some of the brightest and most capable people who could be charged with determining whether we have left doors open and whether the systems are adequate or whether, in effect, we really know all the answers as to how inappropriate access can be obtained.

I guess what I am asking you is: are we as bright within your agencies as the people out there, particularly the younger people who are coming up and know these kind of systems like the back of their hands? Are we as bright as they? And are we as capable as they in understanding what is possible when it comes to entries of access?

Mr. FRAZIER. Let me comment on that on a number of levels. First, I think that we recognize the need to go out and get new talent, if you will, to stay current with this. We are using contractors like never before because, as you point out, we cannot literally keep IT specialists. The private sector will hire them away very, very, very quickly.

But at the same time, I am fortunate that I have an assistant IG for systems who I think is one of the best in government. She has brought a lot of people from the private sector, and we have been able to keep them.

It is not easy, you know, but I think that that is something that we have worked very hard to do.

But I think that even more important is for managers to recognize that it is not just about the IT specialist or the security specialist. It is about program officials taking responsibility for this.

You know, you used the term "weakest link," and it is exactly the word that describes the problem. I can put in the best system. I can hire the best people. I can get the best contractors, but then if I get an employee who decides that he or she is going to leave his system on overnight so that a cleaning person can access the system, as we found in one case, then it does not matter that I have hired the best and the brightest.

So the goal here, I think, is to get managers in the Department of Commerce involved. That is why we are so impressed with the Secretary's recent memo that said to the Under Secretaries and others: This is your responsibility.

When we issue our reports to the CIO or if I issue my report to the Director of Security, I am preaching to the choir at that point, but the reality is that I've got to turn around and talk to the people who run those systems, who do not understand, who do not see that information security is their responsibility.

It is an awareness program. I have to tell you when you go in and you brief many senior officials and you start to talk about security reviews and doing quarterly reviews, their eyes kind of gloss over because it sounds so boring or that is "not my responsibility."

Quite the contrary, it is something that has not been taken seriously in the past, and until all of us, until everyone recognizes the role that they are charged with playing, I think that we are going to come back to you year in and year out with the same kinds of problems. That is my frustration.

Chairman TAUZIN. Very well said.

Thank you, Mr. Chairman.

Mr. GREENWOOD. I thank the chairman of the full committee for his participation and note that with his heavy schedule and six subcommittees to cover, it is impressive that he manages to come to each one of our hearings and spend the time. We appreciate it.

The Chair recognizes the gentleman, Mr. Burr, to inquire.

Mr. BURR. Thank you, Mr. Chairman.

Mr. Dacey, I have seen a lot of folks behind you going like this. So I assume that they are part of the security analysis team, and let me thank them for their good work.

But let me ask you a real important question. Are they the best that is out there?

I think we have a very good team actually, whether they are behind me or not.

Mr. BURR. And I am sure you do, and I thought of another way to ask it, and I could not think of it, but the likelihood is there is somebody out there that is going to be as good if not better.

Mr. DACEY. Our aggregate experience averages about 20 years per person on our staff doing this work at this point in time.

Mr. BURR. Well, then you may have the best.

Mr. DACEY. No, I do not profess we have the best. I do not think they would profess that, but we have some good folks here.

The issues are in this whole environment that there are a lot of people who are out there that are finding these vulnerabilities and issues with systems that apparently have the time and abilities to go do that. We do not try to discover new ones. We just try to figure out if agencies have processes in place to find them and fix them, and that has been a challenge, and we have pursued that role to try to do that.

Mr. BURR. The question that I am trying to get answered: there are a host of folks in the world who have skills at least equal to the folks that conducted this review of the deficiencies and security at Commerce. Would that be safe to say?

Mr. DACEY. Yes.

Mr. BURR. So we have got an ever looming threat of people who want to get into these systems. Now, I would assume that commerce is probably linked to the Department of Energy, and if one could hack into Commerce, they might find their way at least to try to get into the Department of Energy, and if the Department of Energy had an area that might have a deficiency and they got into that, the Department of Energy is linked to the nuclear labs, and you follow the path I am going, that one could enter in Commerce and potentially end up in the Los Alamos system.

Is that conceivable?

Mr. DACEY. We really did not look at that connectivity, but if, in fact——

Mr. BURR. If they were connected.

Mr. DACEY. And if it was not adequately controlled, yes, that is conceivable, but again, given the particular facts I do not know. We did not look at the interconnectivity of Commerce to other bureaus.

So it is an issue, but I think it is one that has not been actively explored, and that is not just Commerce, but the interconnectivity between various bureaus. I mean there is some of that interconnectivity. When we do our work, we find connections to other bureaus routinely.

We have not tested those because our work has typically been focused on the bureau that we have been looking at at that time.

Mr. BURR. And we know that employees of Commerce are paid by the United States Treasury. Therefore, there is probably a link to the Treasury, and because there is a link to the Treasury, the Treasury is probably linked to every other agency, and there might

be a way to go that system and test numerous different agencies within the Federal Government.

Mr. DACEY. It depends on the connectivity and the controls. In some cases, for example, the information may, in fact, be just downloaded and pushed down to another entity. There may not be a live connection, and there are a lot of other things that go on.

So I think though that that is an increasing risk because what we are seeing overall is more interconnectivity as time goes on. It is certainly convenient, and it saves time and cost.

At the same time, there need to be adequate controls in place to prevent someone from doing what you suggested.

Mr. BURR. And am I correct that a scenario like that could happen if you had one entry point that they could get into?

Mr. DACEY. In the situation, take Commerce, for example. As I said, some of our access to this sensitive data was obtained through other bureaus. So we were able to get in.

Typically that is what we do. As I said before, we do not explore every conceivable opportunity to get into the systems because when we find one and gain the level of access we obtained——

Mr. BURR. You are completed.

Mr. DACEY. [continuing] we do not need to go further to do what we do.

So there are definitely weakest link concepts that we talked about earlier that need to be protected against.

I would also like to reiterate that most of our testing that we have done here is technical in nature. We have tools that are available to virtually anyone that can identify these types of vulnerabilities and tools to exploit them.

What we have not done much of, one thing that the hacker community does, is something called social engineering, where they try to gain information like passwords and other information from employees, which is why employee awareness is very important as we talked about earlier.

And so those are the issues. The weakest link might be someone answering a phone and saying, "Yes, here is my password and user ID," and someone else using it to log onto the system, and if you get a little bit into the door, oftentimes you can get information, including network traffic, that has other passwords and escalate your privileges to the level we seek to obtain.

Mr. FRAZIER. And, in fact, as part of our penetration testing for the financial statements, our CPAs did exactly that, called up, pretended to be the system administrator, told someone that they needed their password to get in, and the person gave it to them over the phone, and so we know that that has, in fact, happened.

Your questions are right on the money. Those are the questions that the system's administrators, that the program officials, and the security people should be asking every day. You should make the assumption that people are constantly trying to get into your system.

And what is important is that you should make the assumption that they are trying to get into your system so that they can get into other parts of the Department of Commerce because you do not know what the interconnectivity is, and so until you do the extensive testing, which is seldom done at any agency, you have to

make that assumption that this is happening on a continuous basis.

Mr. BURR. Let me ask you real directly, Mr. Frazier: do you know all the connectivity point?

Mr. FRAZIER. No. Right off the bat, no.

Mr. BURR. Is there anybody at the Commerce Department that does?

Mr. FRAZIER. And I would venture to say at this point, no.

Mr. BURR. So even if it was not a technical deficiency that we had, a simple password management problem might create access for somebody intending to enter the system and figure out where they can go.

Mr. FRAZIER. Yes.

Mr. BURR. Okay. Let me ask you real quickly. Your testimony seemed to rehash some of the issues covered in the 1999 report your office sent to then Secretary Daley. I believe, in fact, the report had your name on it, if I am correct.

Mr. FRAZIER. Yes, it did.

Mr. BURR. Why should we have confidence in your office's ability to insure needed changes do take place, I guess, considering the fact that you have raised the issue? You have raised the issue. We know it has gone to the level of the Secretary, and we still have a problem.

Mr. FRAZIER. It is an easy answer there. We identify the problems. We then report those problems to managers. We, as you know, report to the Congress also. We come to the Congress and tell them the same story. We send them our list of the top ten challenges.

We sent that report up to the Hill. Unfortunately we have not been empowered with what I call the enforcement tool that says, "You are going to put the resources into this area to develop it."

If you use BXA, for example, you can go back 5 years and find out where the IG's Office—I was not the IG—recommended that that system be improved, that the system be updated. It identified many weaknesses as long ago as 5 years.

In our 1999 report, we found a litany of problems, whereas we have checked recently and found out that about half of those issues have been addressed, but some of the most critical ones, the ones that say are you trying to see if people can penetrate your system, are you regularly developing the kinds of security plans that are required by the government rules and regulations, and the answer is still no.

Now, we have not let that drop because we currently have an inspection team that is in there looking at the ECASS system again. And again we will take the message of our findings to the Congress, to the Secretary, and you hope that they will get the message.

Again, I would go back and emphasize the program officials having the top responsibility for making sure that these are implemented.

We have testified that in the case of BXA, that there should be additional funding to support the resources that were necessary to develop that system, and that's something that an IG usually does not do. We are usually trying to find ways to cut resources.

But in that case, we went on record as saying, yes, we think that that system definitely needed to be upgraded. It needed additional support, and again, that's not an excuse. It says that this is the way it is in the sense that we do not have the authority, if you will, to go in and make somebody do anything.

We can surely use the bully pulpit. That is why I am so pleased with this hearing today because it represents an opportunity for these issues to be aired. In fact, they should have long been done.

Mr. BURR. Well, we hope you will continue to speak very loudly on it and not wait for the invitations from us. I think you have gotten an administration that is very anxious to solve some of these problems.

Both of you in your testimony, I think, alluded to one phrase that I found very interesting, excessive user privileges, and I remember when we were in the heat of the investigation at our nuclear labs. One of the problems that we found was the lack of different levels of security within the lab.

We had adopted this policy in the early 1990's where rather than offend somebody, we sort of brought everybody in at the same status and never thought about the fact that that gave everybody the same type of access to the sensitive areas of a computer system, and that contributed to the potential nightmare that we saw.

Does there exist a separation of individuals' levels of access that they can get in the Commerce system, or once you are in, you are in everything or you are only in a compartmentalized area?

Mr. FRAZIER. It is hard to generalize, but I can tell you examples where that has definitely been a problem in the Department of Commerce, without mentioning the bureau's name, where certain people who should have had the authority, for example, to only read information were inadvertently given the authority to not only read, but to alter the information.

Now, that can have very dire consequences when you give 15 people access to a system that should not have access.

Now, what was equally troubling, of course, when we found this out, the second time what was of great concern to us, if they had done what I call the quarterly monitoring, if they had done the risk assessment, that is something that would have been identified, and again, managers too often think of this as just these requirements that really do not have any impact, and you cannot overemphasize that these are things that are put on the books for a very good reason.

So the answer is yes.

Mr. BURR. Mr. Dacey?

Mr. DACEY. There are different levels of access that one can give to different systems. Our main target in our review is to try to get at the system administrator level of access, which is the one that should be fairly tightly controlled and limited to only a limited number of folks. So there is the ability to do that.

What we found in Commerce though is not a regular review process, as was just discussed, to look at those and see if, in fact, they have been properly allocated to the right people.

Additionally, we also found system administrator passwords and information in files in certain bureaus that would give us that ability. So even if we had not been given the direct access, we could

have gained information that would have allowed us to log on or sign on at that level of access.

Mr. BURR. So that would sort of come under that header of password management problem?

Mr. DACEY. And how is it stored in the system.

Mr. BURR. I will ask one last question. The chairman has been very patient.

Could we at least conclude that if an individual who had a password that allowed them the same access you were able to achieve as an administrator left the Department of Commerce, could we believe that their password would be canceled, altered, or are we convinced that they could not access the system when they left today?

Mr. DACEY. We did not specifically look at that at Commerce. I know in other bureaus it is an issue of people revoking passwords on a timely basis, but I believe the IG has done some work in that area.

Mr. FRAZIER. Yes, there are cases where that does not happen. If you are in the private sector, my brother-in-law works for CISCO, and he points out that when you go in and tell them that you are going to leave, they change your password before you leave the room, terminating your access to the systems.

We have people who have been out of the Department of Commerce for 3 years and who still we found have access to the system.

That is unacceptable, absolutely unacceptable, you know.

Mr. BURR. I thank both of you.

I yield back.

Mr. GREENWOOD. The Chair thanks the gentleman for his inquiry. The gentleman asked if you folks had the expertise. It is my observation that you do not need the smartest hackers in the world to get into a department who has a computer security system that is the cyberspace equivalent of the Keystone Cops.

So I do not think you need to worry about what your capacity is.

Mr. BURR. Mr. Chair, could I say that I think Mr. Dacey has the smartest ones?

Mr. GREENWOOD. Both of you have also found in your respective audits a failure on the part of the Commerce bureaus to prepare risk assessments and security plans for their sensitive systems, including some that have been designated as critical to our national security.

Is this just a paper work problem, or should we be truly concerned about this lack of documented assessments and plans? Either gentlemen.

Mr. FRAZIER. Well, see, I think that therein is part of the problem, is there are too many managers who perceive it as a paper work exercise. This is just another check list for us to go through.

And I cannot overemphasize the importance of changing that thinking, establishing a different culture that says we need to do this, and it needs to be done on a regular basis.

That is part of the problem, and again, I think I mentioned that.

Mr. GREENWOOD. Let me ask this to both gentlemen. We have your official reports and so forth, but I also know that in some of these tests you gave advanced warning to the department that you were going to be doing this testing. I assume you had conversations

with people in the department whose work you were examining and whose job—maybe you did not, but I would be interested in what those informal conversations were like.

I mean, did people in the department say, "Oh, God, you are going to look at our system, and I know you are going to find that it is awful and I am embarrassed," or, "we are doing the best that we can, but we just are overworked. We will get to it?"

When you communicate with folks in the department whose job it is to set up these security systems, what kind of dialog is that? What has that been like?

Mr. FRAZIER. Well, when we do our penetration testing with the CPAs through the financial systems, we usually identify one bureau official who is sworn to secrecy and will work with us, but as I have pointed out, usually once you identify these problems, these are people who are in the systems business, who understand systems, and you are preaching to the choir.

The message has to be conveyed to their supervisors, to the top officials to let them know that they have got to get the message out on a broader level. This is not just a problem for the accountants to worry about or the systems people to worry about or the security people to worry about.

And traditionally that is what happens.

Mr. GREENWOOD. But I am talking about the people in the department whose job it has been to comply with the Federal law and to make sure that these systems are secure. When you communicate with them, have they said, "Our hands are tied. We do not have the resources. We are not well trained enough. I do not have enough people?"

What do they say?

Mr. FRAZIER. A number of things, but, in fact, I think that Bob alluded to the fact also that the department has agreed to implement the recommendations.

We went back in preparation for this hearing and looked at the recommendations that we had issued, say, in the last 2 to 3 years in the areas of IT security, and almost without exception, I mean, let's say if there were 100 recommendations, there may have been 5 to 7 that the bureau said, "We disagree with you on."

So they give you the assurances that they are going to deal with this, and they send in what we call action plans to tell us how they propose to deal with it, but also, if you look at those audit action plans and inspection action plans, usually they raise questions about the limited resources that they have available to implement some of the recommendations.

And then the other thing is that they, too, are faced with the problems of making sure that they have the talent to do this.

Now, you take one bureau. I will not mention the name, that has plenty of resources, and they went out and hired a CPA firm to try and penetrate their system doing the exact same thing that we do or GAO would do, and any bureau can do that.

In fact, most bureaus should have that as part of their risk management plan. So part of it does come down to resources, but, again, it comes down to a commitment.

Mr. GREENWOOD. But when they have complained about inadequacy of resources and they have asked for the resources, did you

get a sense of how far up into the hierarchy? Did those requests go to the Secretary's level? Did the Secretary transmit those requests to the administration?

Where was the weakest link, so to speak, in terms of the folks in the department or in the administration who failed to provide the resources?

Mr. FRAZIER. I send all of my reports to the head of the bureaus, the Under Secretary level or the Assistant Secretary level, and any finding or observation that has IT security implications would have been sent to the department's CIO and to the department's Deputy Assistant Secretary for Security.

So the report, the information has surely been made available.

Mr. GREENWOOD. And the problem, I think—correct me if I am wrong about this—but the CIO has a variety of responsibilities beyond. The security of the IT is a subset of the CIO's responsibilities; is that correct?

Mr. FRAZIER. Yes, that is correct.

Mr. GREENWOOD. Okay, and what were some of the other responsibilities of the CIO?

Mr. FRAZIER. One of the things I looked at, how long we have had IT security on our list of the top ten management challenges, and it has been about 1½ years, and I asked my Assistant IG, "Well, why didn't we have this on there earlier?" Because we knew that there were problems.

And she said, you know, a lot of times we forget that back in 1988 and 1989 most of us were preoccupied with the Y2K issues, which you know, we kind of forget. The concern was whether——

Mr. GREENWOOD. Do you mean 1988 or 1998?

Mr. FRAZIER. I am sorry. 1998.

Mr. GREENWOOD. Nobody was thinking about it in 1988.

Mr. FRAZIER. The concern was whether the systems were going to function literally, and so people were not worried about some of the details.

And the other thing, if the truth be told, is these systems have become more sophisticated and more interconnected. This problem has grown, and I do not think that our interest and attention has kept up with the way that the system technology has grown, and so I think that that is part of the problem.

Mr. GREENWOOD. Mr. Dacey, do you have any other comments?

Mr. DACEY. No. I think it is a matter of emphasis. Some of the things that we have found is that for some of the bureau's security officers, it was a part-time duty. They had other responsibilities even besides security management. They did not have a full-time security manager, even one in some bureaus. I think that is a major issue.

In terms of thoughts, I know they had time to prepare, and I know in the process of doing our work things improved because they were aware we were there and we were certainly fixing issues.

But when we raise these issues, they are generally not a big dispute, and generally the people we talk to appreciate the significance of the vulnerabilities that we highlight. So we do not have a lot of convincing to do.

So the real issue is really focusing attention because I think if it was placed that they would be able to find the same kind of

vulnerabilities that we find and use some of the same tools that we use to do that.

Mr. GREENWOOD. Mr. Frazier, in your financial control audits for fiscal year 2000, you looked at seven Commerce bureaus including NOAA, NIST, the Census Bureau, and others, and found that access control problems existed at all seven locations. Can you be more specific about what you mean by access controls?

Mr. FRAZIER. Well, we looked at the access controls at four of the seven, and what that means is that we were able to get into the system. I mentioned that we were able to get one individual system administrator to compromise his or her password.

We also were able to get into the system in ways that we should not have been able to get into the system, and again, the CPAs use Cybercop and several other readily available software packages to try and do this penetration testing, and so it is not like they have some special techniques that need to be used, but in using what is readily available software, they were able to access these systems.

Mr. GREENWOOD. Do you believe that this represented a material weakness or a reportable condition under the relevant statutory authorities?

Mr. FRAZIER. Well, they were reportable conditions, but of course, once you pull them together and we issued our consolidated reports for the Department of Commerce, we became concerned that it was a material weakness.

Individually it may not have been a material weakness at the various bureaus, but again when pulled together and looked at together, it would be a material weakness.

Mr. GREENWOOD. Okay. A related question, again, for you, Mr. Frazier, and, Mr. Dacey, if you would like to comment, please do.

GAO has testified that at the seven bureaus it reviewed, none of them had effective internal or external network security controls. It appears based on the body of IG audit work at other Commerce bureaus that there is nothing unique about these seven bureaus in this respect, and that in your opinion similar deficiencies either have been or would be found at virtually any commerce bureau.

Would that be a fair statement?

Mr. FRAZIER. Let me clarify one thing. GAO is looking at seven bureaus. We are looking at seven financial data centers. So we are talking about apples and oranges. There would be, for example, one financial data center, such as NOAA, and BXA would be the same one. So it is not the same seven.

So when we talk about what we have found in problems at all of these seven locations, it is not the same seven. Okay?

Mr. GREENWOOD. But the problems are similar.

Mr. FRAZIER. The problems are definitely similar.

Mr. GREENWOOD. And there is no indication that anybody at the department level Commerce-wide had been creating security systems in other bureaus that would make the seven that you looked at unique.

Mr. FRAZIER. I'm sorry?

Mr. GREENWOOD. I am assuming that what you found in these seven bureaus and these seven centers, there is no reason for us to believe that they were unique. One would assume that——

Mr. FRAZIER. If you look at seven and you find——

Mr. GREENWOOD. [continuing] the department as a whole allowed these weaknesses in these seven bureaus, there was nothing going on at the department at the top most level that would have presented these weaknesses in other bureaus.

Mr. FRAZIER. Yes, I do not think so.

Mr. GREENWOOD. Mr. Dacey, any further comments?

Mr. DACEY. No. Just based upon a reading of some of the reports that the IG has issued, the nature of the vulnerabilities appeared to be similar.

Mr. GREENWOOD. Okay. We are about to hear from the new Deputy Secretary. Let me just ask you in his presence if you could make one recommendation, each of you gentlemen, what would be your most critical recommendation to the department?

Mr. FRAZIER. Well, I have had the pleasure of meeting with Deputy Secretary Bodman, and when we sat down at our first meeting, the first thing we talked about were the challenges facing the department. It was a lengthy meeting, and one of the things that I was encouraged about, as you know, he has an engineering background. He comes from the business sector. He comes out of the academic community, and it was very clear that he understands systems.

But more to the point was getting the message out to the program officials to hold them responsible. I think often we look for very complicated fixes, and the point that I surely tried to convey to him, that part of this is an awareness program.

And so there is a short memo that came out that said basically to the secretarial officers: you are now basically responsible for security in your agency.

That will probably have a greater impact than putting an additional $2 million in every budget in the department. I mean if you begin to change that culture.

So I am encouraged, is the word that I use, that I think he will bring a new dimension there.

Chairman TAUZIN. Mr. Chairman.

Mr. GREENWOOD. The Chair recognizes the chairman.

Chairman TAUZIN. Could I be recognized and strike the last word for a second?

Mr. GREENWOOD. The Chair yields to the gentleman.

Chairman TAUZIN. I thank the gentleman.

Mr. Chairman, I have to be at the White House in about 10 minutes for a cabinet meeting on global warming, and so I am going to have to leave right now, and I will not have a chance to visit with the witness from the Commerce Department, but I wanted to put on the record at this point my deep concern about the existence of "cookies" and Web "bugs" within the Commerce Department systems, and my concern that even now that the department is focusing on the existence of these "cookies," that as the testimony indicates are there without a compelling reason and without the approval of the Secretary, that the department's CIO is now recommending a strategy to control the use of persistent "cookies" and Web "bugs."

My concern is that I think we ought to go further than that. My understanding of the policy of the government is that unless there

is a very good reason for a "cookie" or a Web "bug" to exist on Federal sites, that we will have a very serious concern about Americans having to deal with these devices when they are sharing their information, as I said, involuntarily with the government.

I can understand "cookies" and Web "bugs" on commercial sites that I enter voluntarily and choose to visit and do business with, but when American citizens are asked to involuntarily do their business with the government with the Internet only to find that we have permitted someone else, some other institution, perhaps not even a government institution, to be collecting that information for other purposes sometimes without the knowledge or consent of the citizens of this country, that raises grave concerns.

When leader Dick Army and I asked for a study by the GAO of the existence of security and privacy on Federal sites, we were appalled to find out; so was the Senate appalled to find out that there were so many "bugs" on the systems and so many "cookies" that were actually out there. We found one on an IRS site. We found a "cookie" for a private enterprise concern in this country collecting information from citizens on an IRS site.

Now, how abominable is that? It is bad enough having to deal with the IRS, but to think that the IRS is sharing our information with other people without our consent is outrageous.

And so, Mr. Chairman, again, my apologies for having to leave because this is such a good hearing and it is such a serious focus of your oversight investigations work that I hate to leave it, but I want to leave it with this thought, and I hope the department witnesses are prepared to speak out forcefully about their intention about how they intend to deal with these "bugs" and this "cookie" problem.

Americans ought not to have to be surprised to find out that private information is being shared by their own government with people they might not want to share it with. It is as simple as that.

Mr. FRAZIER. As you are aware, we did find 12 of them in the Commerce system, but to the department's credit, the Secretary has hired a special advisor for privacy. He has met with me and my systems people to ask about other particulars.

Chairman TAUZIN. Well, you do not need an expert consultant to tell you that when we have got a Federal Trade Commission that is pounding on private companies in America to have good policies of disclosure to consumers about what they are gathering and how they are using that information, you do not need an expert to tell you there is something deadly wrong about the government doing it without consumers' permission, particularly when it is information, as I said, that we are sharing not necessarily of our own volition.

And if consumers have questions about privacy in the commercial world, I can promise you their concerns rise to astronomical levels when it comes to information they are sharing with the government very often only because they have to.

So anything you can do to put a spotlight on this problem and anything the department can do to help us aggressively stop whoever it is in our government who thinks they have the right to do this without asking our consent as citizens of this country to allow others to come in and gather information about us without our con-

sent, I hope you come down like a sledge hammer in your reports, and I hope the department comes down like a sledge hammer on any employee who thinks they have a right to do that without very important reasons that are well spelled out and well justified and approved at the top and with the disclosure to Congress of what is going on.

And I thank you very much, Mr. Chairman.

Mr. GREENWOOD. I thank the chairman, again, for his participation and for his keen interest in this issue.

And before I recognize Mr. Burr for inquiry, I had a question on the table, to which Mr. Frazier has responded, and before I go to Mr. Dacey, Mr. Frazier made reference to the memo dated July 27 from Donald Evans, the Secretary, on the high priority to information technology security.

The Chair would, without objection, enter it and several other documents provided to us by the department for the official record.

Mr. Dacey, if you would respond to the question about your No. 1 recommendation, then I would following that recognize the gentleman from North Carolina.

Mr. DACEY. I think it is important that a good foundation be established on which to build the future efforts to provide security at Commerce. There is currently an IT restructuring plan for IT overall, as well as a task force focused on computer security, and those groups are to provide recommendations and there are to be developed policies and procedures.

I think in doing so there is an excellent opportunity for the department to put together that strong foundation and support, and they should do so, including clarifying the roles and responsibilities of the various parties for security in the department, including the department-wide CIO, as well as the bureaus' CIOs.

It is also important to provide accountability and make sure those people are accountable for providing security, and also in that process, address the resource issue to insure that there are adequate resources put to bear to address the security issues.

I think now is a critical time to do that, and it is important to proceed in that manner.

Mr. GREENWOOD. Thank you.

Mr. Frazier, were you about to say something?

Mr. FRAZIER. No.

Mr. GREENWOOD. Okay. The Chair recognizes the gentleman from North Carolina.

Mr. BURR. Mr. Chairman, just for clarification if I could, Mr. Frazier, because in my last question you said that there had been instances where former employees' passwords stayed active in you said 3 years. Are there currently any former employees whose passwords are still active?

Mr. FRAZIER. I could not answer that, but I would make the assumption that the answer is yes because it is not something that I have monitored. If someone left yesterday, it is that kind of situation.

The concern is that there is not a system in place that would check that with such regularity to make certain that it could not happen. You know, I could not say that it is, but I would be amazed that it is not.

Mr. BURR. Given your role, has a recommendation been made for a process to be set up to make sure that those passwords are eliminated?

I mean, in the private sector they are eliminated as soon as you utter the words, "I am leaving."

Mr. FRAZIER. Yes.

Mr. BURR. I think one of you alluded to that.

Mr. FRAZIER. That is the recommendation that I would make.

Mr. BURR. It has been made or——

Mr. FRAZIER. It has not been made, but it is interesting because I think I did not think of that until literally this morning. We raised the concern about people who had left, and we brought those to the attention, and we have a recommendation that says, on a bureau-by-bureau basis, that says when someone leaves, the password should be changed.

And the question that I have to go to to look to see if we have elevated that to the CIO's office so that it could become a department-wide policy. It has been made at bureau level.

Mr. BURR. I think you are going to get the answer.

Mr. FRAZIER. Yes, it is at the bureau level as I have suggested. But is surely is one that should be made at the department level.

Mr. BURR. I would hope before the end of the day that recommendation would be made.

I thank you for the information.

Thank you, Mr. Chairman.

Mr. GREENWOOD. The Chair thanks the gentleman and wishes to thank both of the witnesses for your fine work, for your testimony, for your continued cooperation with this subcommittee.

And allow me to thank both of your staff folks, those with you and those not with you, for the excellent service that they provide to the country. This is an issue that is in some ways obscure, but increasingly it becomes evident that this is so critical to our national security and to the confidentiality that our citizens demanded and have a right to, and so we thank you for your work and the work that you will do in the future.

And we excuse you now.

Mr. DACEY. Thank you.

Mr. FRAZIER. Thank you.

Mr. GREENWOOD. And call our next witness, who is the Honorable Samuel W. Bodman, Deputy Secretary for the Department of Commerce. He is accompanied by Mr. Thomas Pyke, the Acting Chief Information Officer.

Welcome, Mr. Secretary. Welcome, Mr. Pyke. Thank you for being with us this morning.

You are aware that the committee is holding an investigative hearing, and when doing so we have had the practice of taking testimony under oath. Do either of you have objection to testifying under oath?

Seeing no objection, 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. BODMAN. No, sir.

Mr. GREENWOOD. The gentlemen indicate negative in that case.

If you would please rise and raise your right hand, I will swear you in.

[Witnesses sworn.]

Mr. GREENWOOD. So swearing, you are under oath, and you may now give your testimony, Mr. Bodman. Thank you, again, for being with us.

TESTIMONY OF HON. SAMUEL W. BODMAN, DEPUTY SECRETARY, ACCOMPANIED BY THOMAS PYKE, ACTING CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF COMMERCE

Mr. BODMAN. Mr. Chairman, I appreciate the opportunity of being here.

I have submitted my formal statement, and I will attempt to summarize it in the interest of time.

I am accompanied today by Mr. Pyke, who is our Acting Chief Information Officer for the department. I will count on him for the answer to any technical questions that may come up, although he took on his role only recently. His background in security, I think, is notable—in particular, his having directed the National Institute of Standards and Technology's program for the development of governmentwide computer security standards and guidelines, which assignment he had prior to his becoming the CIO at NOAA.

And then he was asked recently to take on the acting CIO job for the department as a whole.

I can report to you that Secretary Evans and I are very concerned about the findings that have been reviewed this morning. I am as concerned as the committee, perhaps more so.

I want to thank the committee, and I want to thank the GAO with sincerity, as well as the IG's Office for all of the hard work that they have done on this.

I have had experience in my prior life of having managed IT security systems at both Fidelity and at Cabot Corporation, where I was previously employed. I appreciate the significance of this matter, and I hope that my previous experience will be of some value in dealing with these problems.

Speaking for the Secretary and myself, we accept the findings of the GAO report, both specifically and as to their general causes. I do not have much more to say. The defense stipulates the evidence.

We are here to assure you that we will work hard on dealing with these issues. You have alluded before to some of the actions that the Secretary has already taken to build a strong and effective IT security program.

First, he has directed all of the Commerce agency heads to focus their personal attention on this matter. I think, as the Inspector General alluded to already, at least in the part of his discussion and testimony that I heard when I arrived, that this is really a matter of a general manager's responsibility, not the responsibility of the CIO. This is a general manager's job.

It is my job. It is Secretary Evans' job, not Mr. Pyke's job. We hope to rely on him to help us get this done, but this is our responsibility, and frankly, I am embarrassed to be here in front of you to hear the nature of what we are dealing with.

Mr. GREENWOOD. Mr. Bodman, how long have you been on the job?

Mr. BODMAN. Six days.

Mr. GREENWOOD. You do not need to feel embarrassed yet. We will let you know.

Mr. BODMAN. I am sorry, sir, but that is just the nature of responsibility. We have it. It does not matter how long we have had it. We are here now, and it is our job. To be responsible for something that is in this great a difficulty is not something that I find a great deal of personal comfort in, however long I have been here.

And I know I speak for the Secretary in this matter.

He has ordered a department-wide IT restructuring plan. We referred to that. It features the department's Chief Information Officer.

Mr. PYKE. This oversight function will ensure that appropriate action is taken at the agency level to implement new departmental IT policies.

Mr. BODMAN. In the past the departmental CIO apparently had relatively little management authority. We believe we have fixed that. In the past the policy seems to have stalled at times when it got to the agency heads, who had in their view more important matters. And I believe that the new priority the Secretary has given to IT security will be very helpful.

The plan also gives each of our CIOs the authority to manage IT security, IT planning and operations, and IT capital investment review. This new approach is in sharp contrast to the old way of doing business, and as I said before, I think it will be helpful.

Third, we have established an IT security task force chaired by Mr. Pyke that will work under my personal oversight. The task force will improve our IT security by developing a comprehensive department-wide plan.

The task force is made up of individuals with a lot of expertise in this area, including people from NIST, which has had a governmentwide responsibility in this area in the past.

We have also enlisted assistance from the National Security Agency, and we are grateful to the NSA that they have been forthcoming with personnel to be helpful to us in dealing with these matters.

The new task force is already at work. They have met more than once, and they are working on a fast track to develop an effective security program for the department and to identify actions that we should take.

We have already received some short-term recommendations, and these have been implemented. We are doing the best we can to get on top of the things that can be dealt with immediately and to bring these problems to a much higher level of consciousness among our managers.

Furthermore, the program development task force will address the assessment of risks throughout the department and the means for providing security commensurate with those risks. They will provide a road map for updating our approach to security problems, develop an oversight process with compliance testing as a key component, and plan a department-wide IT security awareness training program.

The task force is also addressing the specific issues that have been identified, including strengthening access controls. You have heard extensive discussion about that. We are working on it.

The problem with this area involves more of a mind set—how everybody in the department feels about his or her responsibility for security. It is a challenge to deal with these matters because security is a personal responsibility, and it is something that is difficult at times.

I would imagine that even the Congressman may find it difficult at times to change your password and make sure that it is updated. This is a natural, human problem. Certainly I find it a pain in the neck to have to change a password and than remember what my password is.

Mr. GREENWOOD. It is impossible for me to do it. That is why I have a 15 year old daughter to take care of that.

Mr. BODMAN. Well, you are way ahead of me, sir.

In any event, it is something that we believe we can and will get started on, and it is that factor that makes it difficult to forecast exactly when we will be done. I guess the truth is we will never be done because this has got to be an ongoing effort.

The Secretary and I are committed to supporting all of these efforts ourselves under the leadership of our agency heads and our CIOs, and we think that we will get there.

And I want to thank you all for this opportunity of coming here and addressing this matter relatively early in my tenure. And I know I speak for the Secretary, since both of us have come from the private sector and have managed publicly owned companies, in saying that we recognize the kind of responsibility we have for the management of these systems and will do our best to get on top of these problems as quickly as we can.

Thank you.

[The prepared statement of Hon. Samuel W. Bodman follows:]

PREPARED STATEMENT OF SAMUEL W. BODMAN, DEPUTY SECRETARY, U.S. DEPARTMENT OF COMMERCE

Good morning, Mr. Chairman. I appreciate this opportunity to discuss the Information Technology Security Audit of the Department of Commerce that was recently conducted by the General Accounting Office (GAO). Accompanying me today is Tom Pyke, Acting Chief Information Officer for the Department. Although Tom took on this role only recently, his information technology (IT) security experience includes directing the National Institute of Standards and Technology's (NIST's) program for the development of government-wide computer security standards and guidelines.

Secretary Evans and I are very concerned about the findings of this GAO review because much of the work of the Department on behalf of our citizens depends on the quality and integrity of our data and IT systems. We thank the Committee and GAO for bringing this serious issue to the attention of the Department's new leadership. Having managed the IT security programs at Fidelity Investments and the Cabot Corporation, I appreciate the critical importance of IT security, and I trust that my management experience in this area will be of some value in meeting the challenges presented by the findings of the GAO review.

Speaking for the Secretary and myself, we accept the findings of the GAO report, as to both the specific weaknesses identified in the audit and their underlying causes. To correct these security problems and prevent future incidents, Secretary Evans is acting to build a strong and effective Commerce IT Security Program and to correct the technical problems identified by the GAO audit.

First, Secretary Evans has directed all Commerce agency heads to focus their personal attention on establishing IT security as a priority. Working in conjunction with their Chief Information Officers, they will allocate necessary resources to as-

sure that the Department's data and IT systems are protected in order to avoid data loss, misuse, or unauthorized access, and to assure the integrity and availability of Commerce data. In this connection, the Secretary has also recently appointed a Senior Advisor for Privacy, another area important to overall IT security.

Second, the Secretary has ordered the implementation of a Department-wide IT restructuring plan. The plan provides the Departmental Chief Information Officer (CIO) with the authority to guide individual agency CIOs as they address IT security problems. This oversight function ensures that appropriate action will be taken at the agency level to implement new Departmental IT policies. In the past, the Departmental CIO apparently had little management authority, and policy often stalled when it reached the agencies. I believe that the new priority given this matter by Secretary Evans and me, our agency heads and our CIOs will produce positive results.

The plan also gives each of our CIOs the authority to manage IT security, IT planning and operations, and IT capital investment review. This new approach is in sharp contrast to the old way of doing business in which CIOs apparently were not key members of the Commerce management team.

Third, Commerce has established an IT Security Task Force, which will work under my personal oversight. This Task Force will improve Commerce IT security by developing a comprehensive, Department-wide IT security program. The Task Force is made up of individuals with expertise in IT security management, including people from NIST, which has a critical Government-wide role in developing standards and guidelines for effective IT security programs. We also have enlisted the assistance of the National Security Agency. We appreciate NSA's willingness to share its institutional knowledge and leadership in this field as part of the Task Force.

The new Task Force is already working on a fast track to develop an effective IT Security Program for the Department and to identify actions that Commerce should take quickly to bolster its IT security posture. These recommendations for short-term action will be made in the context of the Corrective Action Plans already developed by Commerce agencies in response to specific concerns identified in the GAO review.

Furthermore, the program developed by the Task Force will address the assessment of risks throughout the Department and the means for providing security commensurate with those risks. The Task Force will provide a roadmap for updating the Department's IT security policies, develop an oversight process with compliance testing as a key component, and plan a Department-wide IT security awareness training program.

The Task Force is also addressing specific issues, including strengthening access controls for the Department's IT systems, segregating assigned duties consistent with mitigating risk, and developing policies and procedures for authorizing, testing, reviewing and documenting software changes prior to implementation. Special attention is being given to network security, an area the GAO audit singled out in light of the Department's reliance on network connectivity to carry out its mission. The Task Force is designing recovery plans for the Department's sensitive systems; developing a Department-wide IT security incident detection and response process; and looking at other areas essential to a comprehensive Commerce IT Security Program.

The Secretary and I are committed to supporting the efforts of the Commerce IT Security Task Force and to implementing its recommendations throughout the Department. Under the leadership of our agency heads and our CIOs, and guided by the efforts of this Task Force, we are confident that we are moving in the right direction, and that the Department's IT security program will be effective.

Again, thank you for this opportunity to discuss the IT security initiatives underway at the Department of Commerce. Secretary Evans and I appreciate that effective IT security is vital to the Department's mission, and I am pleased that this important issue is among the first I have devoted my time and attention to after having been sworn in last week. I would be pleased to respond to any questions you may have.

Mr. GREENWOOD. Thank you very much, Mr. Bodman.

We are delighted to have you here. We are delighted to see the prompt response to an issue that this subcommittee thinks is crucial to our Nation's security, and we are very optimistic that in the short time you have been here you have recognized this problem, grappled with it, and are prepared, you as well as the Secretary, prepared to move the department in the right direction.

Let me ask you a question. GAO notes in its testimony that IT management at the department has been very decentralized over the years, 14 different data centers, 20 independently managed E-mail systems, hundreds and possibly thousands of separate networks managed by individual bureaus or offices within bureaus and lots of different connections to the Internet, so much so that we are still not sure the department even knows about all of them.

How would the reforms you have discussed this morning address what appears to be one of the fundamental problems preventing the department from implementing an effective security program?

And, Mr. Pyke, if you would like to comment, you can do so as well.

Mr. BODMAN. Well, let me comment generally, and then I will ask Mr. Pyke to give you more factual information.

First of all, I think that is an accurate statement. We have a very formidable task to bring to ground the management of the information systems that currently reside within the Commerce Department.

The Commerce Department is difficult enough to manage because of the highly disparate nature of the various bureaus that reside therein. On top of that, we have a set of systems, most of which are interrelated, that have grown a bit like Topsy over the years and that do not use a common approach.

And so we have had a department-wide effort to try to bring more common systems such that they can be managed in a more reasonable way, and that has been underway for some time.

I will ask Mr. Pyke to speak to that.

So we think that the competence and capability of this task force will enable us to start getting our arms around this issue, but I would be misrepresenting the facts if I were to tell you that we were going to be done in any short period of time. This is a long-time fix, and it will require our attention over many years, and we expect to put a program in place initially led by Mr. Pyke, and I hope led by him for many years, that will deal with it.

Tom, do you want to speak to that?

Mr. GREENWOOD. Let me insert another question, Mr. Pyke, that is related to that so that maybe you can answer both at the same time.

And that is can you describe the number of Commerce personnel in these bureaus and at headquarters that are dedicated to computer security and their level of training and other job duties? So when you talk about what you are going to be able to do, also if you could tell us how well equipped you are in terms of person power.

Mr. PYKE. Thank you, Mr. Chairman.

The CIO management structure that has now been put into place and empowered by the Secretary and the Deputy Secretary, which includes the department level CIO and CIOs for each of the Commerce agencies, is now in the position to get on top of the extensive IT systems and networks that the department has. It is going to take a while to bring the necessary discipline in the area of IT security into the management of all of those systems and networks.

It is important that at the departmental level we provide suitable guidance that is generic and strong guidance that provides a

basis for the individual bureaus or agencies to get moving and to devote the necessary resources to IT security.

As the Deputy Secretary said, the department's mission is broad, and the various agencies have diverse activities. And so it is important that each one of them have a CIO leader who I work very closely with, who is in a position to address the specific kinds of issues relative to IT security and IT management in general, on a continuing basis, that relate to that agency's mission and the kinds of systems they have.

At the present time, we have a very small number of people at the department level devoted to IT security. We are increasing that number of people and the amount of contract support very substantially very fast.

As was mentioned in earlier testimony, basically up until very recently we had a single person and a couple of assistants, and we are moving very fast now to bring on additional people and have already begun doing that.

At the bureau level, some of the bureaus have a significant staff. At NOAA, for example, there are several people, about three government folks and several contractor folks who spend full-time on IT security, and there are dozens of others across the bureau that spend a lot of their time on IT security.

One of the things we are going to be doing is to make sure that each of the bureaus has an appropriate number of individuals who devote their time to IT security and to managing the program and making sure all of the technical processes are in place.

Mr. GREENWOOD. Let me ask you kind of an organizational chart question, a twofold question.

First off, looking at your position, describe if you would all of your responsibilities to the extent that this computer security is a subset of your total duties. Do a similar explanation for us for the CIOs of the different bureaus, and then if you could explain to me, so I am interested in to what extent this is a subset of their duties, and explain to me what is changing, if anything, in terms of your ability to directly command, if you will, activities on the part of the CIOs at the various bureaus.

Mr. PYKE. First, the general role of the CIO at the department level is to oversee all of the department's information technology activities, both its planning, development of policy at the departmental level, providing guidance relative to procedures, standards, and guidelines that need to be administered on a department-wide level, to monitor the compliance of the entire department, all of the bureaus with the policies, with the standards, with the guidelines.

And with regard to IT security, that includes actually conducting compliance testing, including penetration testing of a kind similar to what both GAO and the Inspector General's Office have been doing, and in fact, that function we expect to be carried out also at the Bureau level.

The planning functions of the CIO at the department level, as well as at the bureau level, include systematic review of proposals for new expenditures in IT, budget initiatives, review in terms of all the way from return on investment to consistency with our IT architecture, which guides our planning and guides our implementation of systems, to the plans for operating the systems and plans

for implementing them, and nothing gets through our review without an IT security plan being an integral part of each proposal.

We also carry out control reviews of ongoing information technology projects and programs across the department, and we are involved in evaluating after the fact how development efforts have gone and putting that information in the hands of the bureaus to build on.

So at the department level it is policy, procedures, guidance, compliance testing. At the bureau level the CIOs also are responsible for any specialized policy guidance that is necessary, procedures that may be unique to the bureaus, with oversight of the operations of IT within each of those information technology computer systems and networks within each of the bureaus, and with making sure that the policies and procedures that are provided at the departmental level, and in part, provided on a Federal Government-wide level, are followed.

We expect that the bureau CIOs will include compliance testing as part of their portfolio, too, and so what we will be doing at the departmental level will be to oversee them and, on a sampling basis, analogous to what the IG and what the GAO have been doing——

Mr. GREENWOOD. So it will be your responsibility to make sure the CIOs and the bureaus have the resources they need so that the buck will to some extent stop with you. If a bureau or CIO says, "I am sorry that we are not doing the things that we should be doing. We do not have the resources," that is when they call you back, and then that is when Mr. Bodman decides whether he is embarrassed again.

Mr. PYKE. Yes, except this time we have two things in place. No. 1, we have this strong directive from the top to the agency heads themselves to get on top of IT security and to put the necessary resources into it, and this should be a big help to each of the CIOs and provide their marching orders basically from the top.

Second, you asked about the reporting relationship a moment ago. Each of the CIOs in the bureaus, each of those CIOs have a dual reporting responsibility. They report first to their agency head or the deputy head, and they also report to me. They also report to the Commerce CIO.

And in fact, when it gets to the end of the year, I have a cut at their performance evaluation in collaboration with their line manager. So they receive guidance from the CIO. They receive direction from the CIO. They are evaluated, in part, in their performance through the CIO. And I'm in a position to help them get the resources they need.

But the person in charge of the resources when it comes right down to it is their agency head, and the agency head has now received appropriate direction.

Mr. BODMAN. If I could add.

Mr. GREENWOOD. Please, sir.

Mr. BODMAN. At the risk of contradiction, the buck stops at the Secretary. The buck stops with me, and it is our responsibility, and that is how every general manager must feel in order to make this work.

And this system that has been put in place calls for this dual reporting that Mr. Pyke has referred to quite correctly, and it is the only way that I am aware of, at least from my prior experience, when you have a crucial staff function to have it work, whether it is financial reporting, whether it is safety management, whether it is environmental management. It has to be handled at the local basis with an empowered individual who works for the local management, but who is audited and advised by a central, capable person. That is Mr. Pyke.

And we believe that that dual reporting and that dual responsibility will work, but make no mistake. The ultimate responsibility, sir, is ours.

Mr. GREENWOOD. Very well. I appreciate that.

I would like to ask about the broader question, Mr. Bodman, of critical infrastructure. This will be my last question, and just for your information, we are aware that you have a commitment at noon.

Mr. BODMAN. Thank you, sir.

Mr. GREENWOOD. And we will get you out of here in about 15 minutes at the most.

As I understand it, the department has assigned one person at the headquarters level to work on these critical issues with little or no support or funding to oversee the bureau's efforts to identify, assess, and then fix vulnerabilities in its critical systems.

As you know, the IG issued a report last year on this topic which was critical of the lack of progress from the department's efforts to date. I want to read you some comments that were written by the department's CIO office in response to last year's IG audit of computer security policies and management.

"Given the lack of priority in funding by the Clinton administration in the area of critical infrastructure protection, we must disagree with the IG assertion that using information as security assessments scheduled to be performed on the department's critical infrastructure system would result in more systems being certified while realizing significant savings. In the event that the Bush administration raises the priority of critical infrastructure through the application of funding, we will take advantage of assessments gained through this avenue."

What do you and the Secretary plan to do about this important issue, given that your department has so many systems and assets critical to our national and economic security and the health and safety of our citizens?

Mr. BODMAN. Well, I cannot speak to the views of the previous CIO. I have never met the gentleman.

I can tell you that the approach that we have put in place that I have described will, in fact, deal with these issues. I do believe that these are crucial. I do believe that—I am not quite sure I understood the quote in its entirety, but I do believe that the efforts that we will put in will bear fruit.

In my view this is not so much a matter of additional funding. We may find that we need additional funding, but this is more a matter of priority. This is more a matter of management. This is a matter of placing importance on this function at the proper level so that we can deal with it. That is what this is about.

I do not think it is a matter principally of money, and so we can count heads. We can count dollars, and we may need additional heads and additional dollars, but this is more about the people understanding that this has to be dealt with. This is more a matter of the bureau heads of the bureau CIOs understanding that we will deal with this and that we are going to do it.

Tom, do you want to add?

Mr. GREENWOOD. The Chair recognizes the gentleman from North Carolina to inquire.

Mr. BURR. Mr. Secretary, welcome. Mr. Pyke.

Mr. Secretary, let me thank you for one thing. I have been on the oversight committee for 7 years. You are the first—my memory is not great. I do not know if I could remember my password—but you may be the first; I think you are the first person who has testified who has ever, one, taken responsibility regardless of how long they have been there and, two, not used funding as a reason why it could not be accomplished.

So if you keep those two things in the right perspective, I have more confidence in any answer you can give me that we will make tremendous progress at closing some of the problems that we have got.

Mr. BODMAN. Thank you, sir.

Mr. BURR. Let me ask you two fairly lengthy questions, and my purpose for doing it is that these might be areas that you have not looked at, and I would be remiss if I did not double check with both of you to ask on that short term list. Did password management make it on that list today?

From the conversation I had with Mr. Frazier, is password management now on that very quick to do list?

Mr. BODMAN. Yes, it did. It sure did.

Mr. BURR. Thank you.

Mr. BODMAN. Today it will be done.

Mr. BURR. Let me discuss and focus on BXA for a minute, which is one of the more sensitive bureaus within the department and the subject of negative audits by both the IG and GAO.

The IG issued a report in June 1999 regarding BXA's management of its computer system, particularly the ECASS system, which is the export control licensing system. At that time the IG found that BXA did not have a security plan for the system. The risk assessment was 5 years old, and BXA had not conducted a security review of this system since the last Bush administration, all of which had long been required under Federal law and under the policy directives.

And let me say my understanding of ECASS, given the nature of the licensing process that goes on, is that other agencies with direct interest in that process would be electronically linked: Department of Defense, the State Department, possibly the intelligence community.

I won't ask you to assess whether that system is air gapped in any way, but I would have some belief that it is probably not from some of the things that I have heard today. Therefore, I would think that it is very susceptible to a potential entry point that sends them into some of the most sensitive areas singularly through the ECASS system.

In response to the department's pledge to undertake those efforts promptly, yet as I understand GAO found the same things with respect to the ECASS nearly 2 years later: still no security plan, no risk assessment, and no security review conducted.

Do you know why these issues weren't addressed by now? And how can we be confident that the department will take seriously these issues in the future?

Mr. BODMAN. First, I can tell you that we take it seriously. We take it so seriously that I am going to ask Mr. Pyke to give you a detailed answer rather than my trying to paraphrase what he told me before we walked in here.

Mr. BURR. Thank you.

Mr. PYKE. Mr. Burr, the problems with ECASS and Bureau of Export Administration are being addressed, and they will be addressed even more intensively as get the strengthened IT security program in place. As GAO conducted its audit, as they made specific findings of weaknesses, attempts were made on the spot, in a very short period of time, to correct those specific findings.

The bureau has also prepared and put in place a corrective action plan that has attempted to address, either already in many cases, but certainly very quickly, all of the specific issues that GAO identified.

As a part of the task force effort that we have now put in place at the department level, we are not only looking generically at computer security and all of the elements of a complete program, but we are looking at all of the specific findings of GAO and of the Inspector General over the last 2 to 3 years, to generalize on those, and to provide very quick advice and guidance to the bureaus, including the individuals in BXA responsible for ECASS.

So all of the findings in each of the agencies can be responded to in a general sense by all of the bureaus. All of this is being applied toward ECASS, and I can assure you that attention is being given by the CIO in BXA and by us to the special concerns that have been expressed about ECASS, and some steps have already been made, as I say, some steps, and we will work with them to make sure that things are completely taken care of in an appropriate way and that adequate protection is in place relative to the risks that they are confronted with.

Mr. BURR. I appreciate that answer, and I think you understand the sensitivity of where someone might venture if, in fact, the correct level of security does not exist within that system.

Mr. Bodman, I note that NIST computer security personnel played a prominent role in your new task force, but I cannot help but be concerned about that, given that despite it, its purported role is the government's expert on computer security.

NIST itself fared rather poorly in the recent IG penetration test and was the subject of a repeat finding in 1999 and 2000 regarding the lack of security plans for its system.

In addition, the self-assessments that were performed by the bureau last year revealed that NIST was just as bad, if not worse, than most of the bureaus when it came to complying with the Federal guidelines on computer security, including those that NIST itself had crafted.

Should we be concerned? If we were concerned before this hearing, should we be concerned after this hearing?

Mr. BODMAN. That is not one I am going to burden Mr. Pyke with answering since at one point in his life he was responsible for the information operations at NIST.

Mr. BURR. That is why I directed the question to you.

Mr. BODMAN. I think it is entirely consistent with what we have been saying. This is not a problem with technology. This is a problem with management. This is a problem with priority.

And to the extent that this becomes a matter that the bureau manager feels a responsibility for, then it will be dealt with, and to the extent that it is not something that the bureau leadership feels responsible for, it will not be dealt with because it is not something that the human being naturally does.

This is something that is easily ignored, just given the nature of the fact that we all like to do something. We all have our own jobs. The thing that gives me great pleasure each day is not worrying about my password management. I have other things that I like to do that I am, I think, a little better at since I seem to have difficulty remembering the password from time to time.

And so I think the fact that we are using the technical skills at NIST as a part of this is entirely understandable and bears no relationship to how that particular agency was evaluated with respect to the management of its information.

Mr. BURR. I thank you for that answer.

As a member of this committee, my goal every year is the hope that I will not see the same witnesses on the same issue at any point in the future. That goal has not been fulfilled yet, but I have reason to believe that as it relates to the security issue and you being here, this might be the last time that we have this conversation, unless it is to report on the progress that you have made.

I thank you.

Mr. BODMAN. I thank you, sir.

Mr. BURR. Thank you, Mr. Chairman.

Mr. GREENWOOD. I thank the gentleman.

And on that point, the report on progress, might we expect a report in 6 months from the department as to how you have responded to these issues?

Mr. BODMAN. We would be happy to report, sir, whenever you wish.

Mr. GREENWOOD. Okay. We appreciate that.

Again, thank you for your presence, for your testimony, for your good work. Welcome to Washington, and we look forward to working with you on a number of issues.

Thank you again.

Mr. BODMAN. Thank you very much.

Mr. GREENWOOD. This hearing is adjourned.

[Whereupon, at 11:45 a.m., the subcommittee was adjourned.]

[Additional material submitted for the record follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at
9:30 a.m. EDT
Friday,
August 3, 2001

INFORMATION SECURITY

Weaknesses Place Commerce Data and Operations at Serious Risk

Statement of Robert F. Dacey
Director, Information Security Issues

GAO-01-1004T

Mr. Chairman and Members of the Committee:

I am pleased to be here today to discuss our analysis of the information security controls over unclassified systems of the Department of Commerce (Commerce). 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, bringing vast amounts of information and myriad resources and activities literally at our fingertips. However, along with the enormous benefits it brings, this widespread interconnectivity poses significant risks to our computer systems, and more important, to the critical operations and infrastructures they support.

As with other organizations, Commerce relies extensively on computerized systems and electronic data to support its mission. Moreover, Commerce generates and disseminates some of the nation's most important economic information that is of paramount interest to U.S. businesses, policymakers, and researchers. Accordingly, the security of its systems and data is essential to avoiding disruption in critical operations, data tampering, fraud, and inappropriate disclosure of sensitive information. Further, there has be a dramatic rise in the number and sophistication of cyberattacks on federal information systems. My testimony today specifically focuses on the effectiveness of Commerce's (1) logical access controls and other information

system controls over its computerized data,[1] (2) incident detection and response capabilities,[2] and (3) information security management program and related procedures.[3] We reviewed Commerce's information security controls and currently have a draft report at Commerce for comment.

At the seven Commerce organizations we reviewed,[4] significant and pervasive computer security weaknesses exist that place sensitive Commerce systems[5] at serious risk. Using readily available software and common techniques, we demonstrated the ability to penetrate sensitive Commerce systems from both inside Commerce and remotely, such as through the Internet. Individuals, both within and outside Commerce, could gain unauthorized access to these systems and read, copy, modify, and delete sensitive economic, financial, personnel, and confidential business data. Moreover, intruders could disrupt the operations

[1] Logical access controls are controls designed to protect computer resources from unauthorized modification, loss, or disclosure, specifically those controls that prevent or detect unauthorized access to sensitive data and programs that are stored or transmitted electronically.

[2] Incident detection is the process of identifying that an intrusion has been attempted, is occurring, or has occurred. Incident response is an action or series of actions constituting a reply or reaction against an attempted or successful intrusion.

[3] Because of the sensitivity of specific weaknesses, we do not discuss them here, but plan to issue a report designated for "Limited Official Use," which describes in more detail the logical access control weaknesses identified.

[4] The Commerce organizations we reviewed were the Office of the Secretary, the Bureau of Export Administration, the Economic Development Administration, the Economics and Statistics Administration, the International Trade Administration, the Minority Business Development Agency, and the National Telecommunications and Information Administration. For the sake of simplification, throughout this testimony, we use the term "bureaus" to refer to all seven of the Commerce organizations, although the Office of the Secretary is not actually a bureau.

[5] By "sensitive" systems we refer to the systems that Commerce has defined as critical to the mission of the Department as well as systems that fit OMB Circular A-130, Appendix III, criteria for requiring special protection.

of systems that are critical to the mission of the department. Additionally, unauthorized access to sensitive systems may not be detected in time to prevent or minimize damage. The underlying cause for the numerous weaknesses we identified was the lack of an effective program to manage information security.

We identified vulnerabilities in four key areas in the bureaus we reviewed:

- First, controls intended to protect information systems and critical data from unauthorized access are ineffectively implemented, leaving sensitive systems highly susceptible to intrusions or disruptions. Specifically,
  - Systems were either not configured to require passwords—including powerful systems administrator accounts—or, if passwords were required, they were relatively easy to guess, such as the word "password" or commonly known default passwords supplied by vendors. Further, (1) a significant number of passwords never expired, (2) individuals had unlimited attempts to guess passwords, and (3) unencrypted passwords, including those having powerful system administrator functions, could be widely viewed. Commerce bureaus also granted excessive system administration privileges to employees who did not require them, including 20 individuals who had powerful system privileges that should be used only in exceptional circumstances, such as recovery from a power failure.

- The configuration of Commerce operating systems exposed excessive amounts of system information to anyone, without the need for authentication, allowing potential attackers to collect systems information that could be used to circumvent security controls and gain unauthorized access. In addition, Commerce did not properly configure operating systems to ensure that they would be available to support bureau missions or prevent the corruption of important data. For example, in a large computer system affecting several bureaus, thousands of important programs had not been assigned unique names, which could result in unintended programs being inadvertently run, potentially corrupting data or disrupting system operations. In this same system, because critical parts of the operating system were shared by the test and production systems, changes in either system could corrupt or shut down the other system. Additionally, unnecessary and poorly configured system functions existed on important computer systems in all bureaus we reviewed, allowing us to gain access from the Internet.

- None of the Commerce bureaus reviewed had effective external and internal network security controls. Our testing demonstrated that individuals, both within and outside Commerce, could compromise external and internal security controls to gain extensive unauthorized access to the department's networks and systems. We obtained such access as a result of weakly

configured external control devices, poorly controlled dial-up modems, and ineffective internal network controls.

- Second, we found other control weaknesses, including inadequate (1) segregation of computer duties of the staff to mitigate the risk of errors or fraud, (2) control of software changes to ensure that only authorized and fully tested software is placed in operation, and (3) development of comprehensive and completed recovery plans to ensure the continuity of service in the event of a service disruption.

- Third, Commerce is not adequately (1) preventing intrusions before they occur, (2) detecting intrusions as they occur, (3) responding to successful intrusions, or (4) reporting intrusions to staff and management. Thus, there is little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage. For example, Commerce has not instituted key measures to prevent incidents, such as acquiring software updates to correct known vulnerabilities. During our testing we discovered 20 systems with known vulnerabilities for which patches were available but not installed. As a result of ineffective detection capabilities, the tested bureaus were generally unable to detect our extensive intrusion activities (only two of the bureaus had installed intrusion detection systems). Also, only one of the bureaus has established incident response procedures; in two instances when our activity was detected, Commerce employees who

detected our testing inappropriately responded by launching attacks against our systems. Moreover, these two incidents were never reported to the bureaus' security officer.

- Fourth, and most important, Commerce does not have an effective departmentwide information security management program to ensure that sensitive data and critical operations are adequately addressed and that appropriate security controls are in place to protect them. Key issues include

  - **Lack of a strong centralized management function to oversee and coordinate departmentwide security-related activities.** At the time of our review, Commerce's CIO, who had broad responsibility for information security throughout the department, said that he believed that he did not have sufficient resources or the authority to implement this program. This lack of a centralized approach to managing security is particularly risky considering the widespread interconnectivity of Commerce's systems.

  - **Widespread lack of risk assessment.** Commerce is doing little to understand and manage risks to its systems. For example, as of March 2001, of the bureaus' 94 sensitive systems we reviewed, 91 did not have documented risk assessments, 87 had no security plans, and none were

authorized[6] for processing by Commerce management. Consequently, most of the bureaus' systems are being operated without considering the risks associated with their immediate environment. Moreover, several bureau officials acknowledged that they had not considered how vulnerabilities in systems that interconnected with theirs could undermine the security of their own systems.

- **Significantly outdated and incomplete information security policies.** Commerce's information security policy, developed in 1993 and partially revised in 1995, does not reflect current federal requirements for managing computer security on a continuing basis, developing security plans, authorizing processing, providing security awareness training, or performing system reviews. Moreover, Commerce has not updated its policy to reflect the risks of Internet use and has no policies establishing baseline security requirements for all systems. For example, there is no policy specifying required attributes for passwords, such as minimum length and the inclusion of special characters.

- **Inadequately promoted security awareness and training.** Although each of the seven bureaus reviewed have informal programs in place, none have

[6] Authorization is the acceptance of risk by management, resulting in a formal approval for the system to become operational or remain so after significant system changes have been made.

documented computer security training procedures that meet federal requirements for ensuring that security risks and responsibilities are understood by all managers, users, and system administrators.

- **Lack of an ongoing program to test and evaluate security controls.** No oversight reviews of the Commerce bureaus' systems have been performed by the staff of Commerce's information security program. Furthermore, the bureaus we reviewed do not monitor the effectiveness of their information security. Only one of the bureaus has performed isolated tests of its systems.

The lack of an effective information security program is exacerbated by Commerce's highly interconnected computing environment in which the vulnerabilities of individual systems affect the security of systems in the entire department. A compromise in a single poorly secured system can undermine the security of the multiple systems that connect to it.

In the last 2 years, the Commerce CIO introduced several initiatives to improve the security posture of the department, including a summary evaluation of information security based on bureau self-assessments and related follow-up. Also, in June 2001, after our fieldwork was completed, the Secretary of Commerce approved a high-level Commerce information technology (IT) restructuring plan. The acting CIO stated that Commerce is developing a more detailedrestructuring implementationplan plan. Regardless of its particular

approach, we have made recommendations that Commerce needs to implement in order to address the weaknesses in its information security controls.

In the rest of my statement today, I will discuss in more detail the results of our review of Commerce's information security controls; these results are included in our draft report, which also contains more detailed recommendations.

Background

Information security is an important consideration for any organization that depends on information systems to carry out its mission. The dramatic expansion in computer interconnectivity and the exponential increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. However, risks are significant, and they are growing. The number of computer security incidents reported to the CERT Coordination Center® (CERT/CC)[7] rose from 9,859 in 1999 to 21,756 in 2000. For the first 6 months of 2001, the number reported was 15,476.

As the number of individuals with computer skills has increased, more intrusion or "hacking" tools have become readily available and relatively easy to use. A

[7] CERT Coordination Center® is a center of Internet security expertise located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT Coordination Center® is registered in the U.S. Patent and Trademark Office.

potential hacker can literally download tools from the Internet and "point and click" to start a hack. According to a recent National Institute of Standards and Technology (NIST) publication, hackers post 30 to 40 new tools to hacking sites on the Internet every month. The successful cyber attacks against such well-known U.S. e-commerce Internet sites as eBay, Amazon.com, and CNN.com by a 15-year old "script kiddie"[8] in February 2000 illustrate the risks. Without proper safeguards, these developments make it easier for individuals and groups with malicious intentions to gain unauthorized access to systems and use their access to obtain sensitive information, commit fraud, disrupt operations, or launch attacks against other organizations' sites.

Federal Systems Are At Risk

Government officials are increasingly concerned about federal computer systems, which process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal operations. The federal government's systems are riddled with weaknesses that continue to put critical operations at risk. Since October 1998, the Federal Computer Incident Response Center's (FedCIRC)[9] records have shown an increasing trend in the number of attacks

[8] The term "script kiddie" is used within the hacker community in a derogatory manner to refer to a hacker with little computer knowledge and few abilities who breaks into systems using scripts posted to the Internet by more skilled hackers.

[9] FedCIRC, a component of the General Service Administration's Technology Service, is the central coordinating activity for reporting security related incidents affecting computer systems within the federal government's civilian agencies and departments.

targeting government systems. In 1998 FedCIRC documented 376 incidents affecting 2,732 federal civilian systems and 86 military systems. In 2000, the number of attacks rose to 586 incidents affecting 575,568 federal systems and 148 of their military counterparts. Moreover, according to FedCIRC, these numbers reflect only reported incidents, which it estimates do not include as many as 80 percent of actual security incidents. According to FedCIRC, 155 of the incidents reported in 2000, which occurred at 32 agencies, resulted in what is known as a "root compromise."[11] For at least five of the root compromises, government officials were able to verify that access to sensitive information had been obtained.

How well federal agencies are addressing these risks is a topic of increasing interest in the executive and legislative branches. In January 2000, President Clinton issued a *National Plan for Information Systems Protection*[12] and designated computer security and critical infrastructure protection a priority management objective in his fiscal year 2001 budget. The new administration, federal agencies, and private industry have collaboratively begun to prepare a

[11] A "root compromise" of a system gives the hacker the power to do anything that a systems administrator could do, from copying files to installing software such as "sniffer" programs that can monitor the activities of end users.

[12] *Defending America's Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialogue.*

new version of the national plan that will outline an integrated approach to computer security and critical infrastructure protection.

The Congress, too, is increasingly interested in computer security, as evidenced by important hearings held during 1999, 2000, and 2001 on ways to strengthen information security practices throughout the federal government and on progress at specific agencies in addressing known vulnerabilities. Furthermore, in October 2000, the Congress included government information security reform provisions in the fiscal year 2001 National Defense Authorization Act. These provisions seek to ensure proper management and security for federal information systems by calling for agencies to adopt risk management practices that are consistent with those summarized in our 1998 *Executive Guide.*[13] The provisions also require annual agency program reviews and Inspector General (IG) evaluations that must be reported to the Office of Management and Budget (OMB) as part of the budget process.

The federal CIO Council and others have also initiated several projects that are intended to promote and support security improvements to federal information systems. Over the past year, the CIO Council, working with NIST, OMB, and us, developed the Federal Information Technology Security Assessment

[13] *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

Framework.[14] The framework provides agencies with a self-assessment methodology to determine the current status of their security programs and to establish targets for improvement. OMB has instructed agencies to use the framework to fulfill their annual assessment and reporting obligations.

Since 1996, our analyses of information security at major federal agencies have shown that systems are not being adequately protected. Our previous reports, and those of agency IGs, describe persistent computer security weaknesses that place a variety of critical federal operations at risk of inappropriate disclosures, fraud, and disruption.[15] This body of audit evidence has led us, since 1997, to designate computer security as a governmentwide high-risk area.[16]

Our most recent summary analysis of federal information systems found that significant computer security weaknesses had been identified in 24 of the largest federal agencies, including Commerce.[17] During December 2000 and January 2001, Commerce's IG also reported significant computer security weaknesses in several of the department's bureaus and, in February 2001, reported

[14] *Federal Information Technology Security Assessment Framework*, November 28, 2000.

[15] *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

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

[17] *Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies* (GAO/AIMD-00-295, September 6, 2000).

information security as a material weakness affecting the department's ability to produce accurate data for financial statements.[18] The report stated that there were weaknesses in several areas, including entitywide security management, access controls, software change controls, segregation of duties, and service continuity planning. Moreover, a recent IG assessment of the department's information security program found fundamental weaknesses in the areas of policy and oversight.[19] Also, the IG designated information security as one of the top ten management challenges for the department.

Commerce Missions Are Diverse

Commerce's missions are among the most diverse of the federal government's cabinet departments, covering a wide range of responsibilities that include observing and managing natural resources and the environment; promoting commerce, regional development, and scientific research; and collecting, analyzing, and disseminating statistical information. Commerce employs about 40,000 people in fourteen operating bureaus with numerous offices in the U.S. and overseas, each pursuing disparate programs and activities.

IT is a critical tool for Commerce to support these missions. The department spends significant resources—reportedly over $1.5 billion in fiscal year 2000—

[18] *Department of Commerce's Fiscal Year 2000 Consolidated Financial Statements,* Inspector General Audit Report No. FSD-12849-1-0001 (February 2001).

on IT systems and services. As a percentage of total agency expenditures on IT, Commerce ranks among the top agencies in the federal government, with 17 percent of its $9-billion fiscal year 2000 budget reported as spent on IT.

A primary mission of Commerce is to promote job creation and improved living standards for all Americans by furthering U.S. economic growth, and the seven bureaus we reviewed support this mission through a wide array of programs and services. Commerce uses IT to generate and disseminate some of the nation's most important economic information. The International Trade Administration (ITA) promotes the export of U.S. goods and services—which amounted to approximately $1.1 trillion in fiscal year 2000. Millions of American jobs depend on exports, and with 96 percent of the world's consumers living outside U.S. borders, international trade is increasingly important to supporting this mission. The Economics and Statistics Administration (ESA) develops, prepares, analyzes, and disseminates important indicators of the U.S. that present basic information on such key issues as economic growth, regional development, and the U.S. role in the world economy. This information is of paramount interest to researchers, business, and policymakers.

[19] *Office of the Chief Information Officer: Additional Focus Needed on Information Technology Security Policy and Oversight* (Inspection Report No. OSE-13573/March 2001).

The Bureau of Export Administration (BXA), whose efforts supported sales of approximately $4.2 billion in fiscal year 1999, assists in stimulating the growth of U.S. exports while protecting national security interests by helping to stop the proliferation of weapons of mass destruction. Sensitive data such as that relating to national security, nuclear proliferation, missile technology, and chemical and biological warfare reside in this bureau's systems.

Commerce's ability to fulfill its mission depends on the confidentiality, integrity, and availability of this sensitive information. For example, export data residing in the BXA systems reflect technologies that have both civil and military applications; the misuse, modification, or deletion of these data could threaten our national security or public safety and affect foreign policy. Much of these data are also business proprietary. If it were compromised, the business could not only lose its market share, but dangerous technologies might end up in the hands of renegade nations who threaten our national security or that of other nations.

Commerce's IT Infrastructure Is Decentralized

Commerce's IT infrastructure is decentralized. Although the Commerce IT Review Board approves major acquisitions, most bureaus have their own IT budgets and act independently to acquire, develop, operate, and maintain their own infrastructure. For example, Commerce has 14 different data centers,

diverse hardware platforms and software environments, and 20 independently managed e-mail systems. The bureaus also develop and control their own individual networks to serve their specific needs. These networks vary greatly in size and complexity. For example, one bureau has as many as 155 local area networks and 3,000 users spread over 50 states and 80 countries. Some of these networks are owned, operated, and managed by individual programs within the same bureau.

Because Commerce does not have a single, departmentwide common network infrastructure to facilitate data communications across the department, the bureaus have established their own access paths to the Internet, which they rely on to communicate with one another. In April 2001, the department awarded a contract for a $4 million project to consolidate the individual bureaus' local area networks within its headquarters building onto a common network infrastructure. However, until this project is completed, each of the bureaus is expected to continue to configure, operate, and maintain its own unique networks.

Improvements to Information Security Have Been Initiated

Recognizing the importance of its data and operations, in September 1993 Commerce established departmentwide information security policies that defined and assigned a full set of security responsibilities, ranging from the

department level down to individual system owners and users within the bureaus. Since 1998, the Commerce CIO position has been responsible for developing and implementing the department's information security program. An information security manager, under the direction of the CIO's Office of Information Policy, Planning, and Review, is tasked with carrying out the responsibilities of the program. The CIO's responsibilities for the security of classified systems has been delegated to the Office of Security.

In the last 2 years, the CIO introduced several initiatives that are essential to improving the security posture of the department. After a 1999 contracted evaluation of the bureaus' security plans determined that 43 percent of Commerce's most critical assets did not have current information system security plans, the CIO issued a memorandum calling for the bureaus to prepare security plans that comply with federal regulations. Also, in May 2000, the Office of the CIO performed a summary evaluation of the status of all the bureaus' information security based on the bureaus' own self-assessments. The results determined that overall information security program compliance was minimal, that no formal information security awareness and training programs were provided by the bureaus, and that incident response capabilities were either absent or informal. The Commerce IG indicated that subsequent meetings between the Office of the CIO and the bureaus led to improvements. The Office of the CIO plans to conduct another evaluation this year and, based on a

comparison with last year's results, measure the bureaus' success in strengthening their security postures.

Finally, for the past year, the CIO attempted to restructure the department's IT management to increase his span of control over information security within the bureaus by enforcing his oversight authority and involvement in budgeting for IT resources. However, this initiative was not approved before the CIO's resignation in 2001. In June 2001, after our fieldwork was completed, the Secretary of Commerce approved a high-level Commerce IT restructuring plan. The acting CIO stated that a task force is developing a more detailed implementation plan.

Logical Access Controls Were Inadequate

A basic management objective for any organization is the protection of its information systems and critical data from unauthorized access. Organizations accomplish this objective by establishing controls that limit access to only authorized users, effectively configuring their operating systems, and securely implementing networks. However, our tests identified weaknesses in each of these control areas in all of the Commerce bureaus we reviewed. We demonstrated that individuals, both external and internal to Commerce, could compromise security controls to gain extensive unauthorized access to Commerce networks and systems. These weaknesses place the bureaus'

information systems at risk of unauthorized access, which could lead to the improper disclosure, modification, or deletion of sensitive information and the disruption of critical operations. As previously noted, because of the sensitivity of specific weaknesses, we plan to issue a report designated for "Limited Official Use," which describes in more detail each of the computer security weaknesses identified and offers specific recommendations for correcting them.

System Access Controls Were Weak

Effective system access controls provide mechanisms that require users to identify themselves and authenticate[30] their identity, limit the use of system administrator capabilities to authorized individuals, and protect sensitive system and data files. As with many organizations, passwords are Commerce's primary means of authenticating user identity. Because system administrator capabilities provide the ability to read, modify, or delete any data or files on the system and modify the operating system to create access paths into the system, such capabilities should be limited to the minimum access levels necessary for systems personnel to perform their duties. Also, information can be protected by using controls that limit an individual's ability to read, modify, or delete information stored in sensitive system files.

[30] Authenticating is the process of verifying that a user is allowed to access a system or an account.

User ID and Password Management Controls Were Not Effective

One of the primary methods to prevent unauthorized access to information system resources is through effective management of user IDs and passwords. To accomplish this objective, organizations should establish controls that include requirements to ensure that well-chosen passwords are required for user authentication, passwords are changed periodically, the number of invalid password attempts is limited to preclude password guessing, and the confidentiality of passwords is maintained and protected.

All Commerce bureaus reviewed were not effectively managing user IDs and passwords to sufficiently reduce the risk that intruders could gain unauthorized access to its information systems to (1) change system access and other rules, (2) potentially read, modify, and delete or redirect network traffic, and (3) read, modify, and delete sensitive information. Specifically, systems were either not configured to require passwords or, if passwords were required, they were relatively easy to guess. For example,

- powerful system administrator accounts did not require passwords, allowing anyone who could connect to certain systems through the network to log on as a system administrator without having to use a password,
- systems allowed users to change their passwords to a blank password, completely circumventing the password control function,

- passwords were easily guessed words, such as "password,"
- passwords were the same as the user's ID, and
- commonly known default passwords set by vendors when systems were originally shipped had never been changed.

Although frequent password changes reduce the risk of continued unauthorized use of a compromised password, systems in four of the bureaus reviewed had a significant number of passwords that never required changing or did not have to be changed for 273 years. Also, systems in six of the seven bureaus did not limit the number of times an individual could try to log on to a user ID. Unlimited attempts allow intruders to keep trying passwords until a correct password is discovered.

Further, all Commerce bureaus reviewed did not adequately protect the passwords of their system users through measures such as encryption, as illustrated by the following examples:

- User passwords were stored in readable text files that could be viewed by all users on one bureau's systems.
- Files that store user passwords were not protected from being copied by intruders, who could then take the copied password files and decrypt user

passwords. The decrypted passwords could then be used to gain unauthorized access to systems by intruders masquerading as legitimate users.

- Over 150 users of one system could read the unencrypted password of a powerful system administrator's account.

Control of System Administration Functions Was Not Adequate

System administrators perform important functions in support of the operations of computer systems. These functions include defining security controls, granting users access privileges, changing operating system configurations, and monitoring system activity. In order to perform these functions, system administrators have powerful privileges that enable them to manipulate operating system and security controls. Privileges to perform these system administration functions should be granted only to employees who require such privileges to perform their responsibilities and who are specifically trained to understand and exercise those privileges. Moreover, the level of privilege granted to employees should not exceed the level required for them to perform their assigned duties. Finally, systems should provide accountability for the actions of system administrators on the systems.

However, Commerce bureaus granted the use of excessive system administration privileges to employees who did not require such privileges to perform their responsibilities and who were not trained to exercise them. For

example, a very powerful system administration privilege that should be used only in exceptional circumstances, such as recovery from a power failure, was granted to 20 individuals. These 20 individuals had the ability to access all of the information stored on the system, change important system configurations that could affect the system's reliability, and run any program on the computer. Further, Commerce management also acknowledged that not all staff with access to this administrative privilege had been adequately trained.

On other important systems in all seven bureaus, system administrators were sharing user IDs and passwords so that systems could not provide an audit trail of access by system administrators, thereby limiting accountability. By not effectively controlling the number of staff who exercise system administrator privileges, restricting the level of such privileges granted to those required to perform assigned duties, or ensuring that only well-trained staff have these privileges, Commerce is increasing the risk that unauthorized activity could occur and the security of sensitive information be compromised.

Access to Critical Systems and Sensitive Data Files Was Not Adequately Restricted

Access privileges to individual critical systems and sensitive data files should be restricted to authorized users. Not only does this restriction protect files that may contain sensitive information from unauthorized access, but it also provides another layer of protection against intruders who may have

successfully penetrated one system from significantly extending their unauthorized access and activities to other systems. Examples of access privileges are the capabilities to read, modify, or delete a file. Privileges can be granted to individual users, to groups of users, or to everyone who accesses the system.

Six of the seven bureaus' systems were not configured to appropriately restrict access to sensitive system and/or data files. For example, critical system files could be modified by all users to allow them to bypass security controls. Also, excessive access privileges to sensitive data files such as export license applications were granted. Systems configured with excessive file access privileges are extremely vulnerable to compromise because such configurations could enable an intruder to read, modify, or delete sensitive system and data files, or to disrupt the availability and integrity of the system.

Operating Systems Were Ineffectively Secured

Operating system controls are essential to ensure that the computer systems and security controls function as intended. Operating systems are relied on by all the software and hardware in a computer system. Additionally, all users depend on the proper operation of the operating system to provide a consistent and reliable processing environment, which is essential to the availability and reliability of the information stored and processed by the system.

Operating system controls should limit the extent of information that systems provide to facilitate system interconnectivity. Operating systems should be configured to help ensure that systems are available and that information stored and processed is not corrupted. Controls should also limit the functions[21] of the computer system to prevent insecure system configurations or the existence of functions not needed to support the operations of the system. If functions are not properly controlled, they can be used by intruders to circumvent security controls.

Excessive System Information Was Exposed

To facilitate interconnectivity between computer systems, operating systems are configured to provide descriptive and technical information, such as version numbers and system names, to other computer systems and individuals when connections are being established. At the same time, however, systems should be configured to limit the amount of information that is made available to other systems and unidentified individuals because this information can be misused by potential intruders to learn the characteristics and vulnerabilities of that system to assist in intrusions.

[21] Operating system functions are capabilities added to the operating system to support specific processing requirements necessary for the system to perform its intended purpose. Examples of operating system functions include the capability to receive electronic mail, the capability have technical support performed remotely, the capability to transfer data between different types of computer systems, and the capability to have users safely execute powerful programs without granting those users powerful access privileges.

Systems in all bureaus reviewed were not configured to control excessive system information from exposure to potential attackers. The configuration of Commerce systems provided excessive amounts of information to anyone, including external users, without the need for authentication. Our testing demonstrated that potential attackers could collect information about systems, such as computer names, types of operating systems, functions, version numbers, user information, and other information that could be useful to circumvent security controls and gain unauthorized access.

Operating Systems Were Poorly Configured

The proper configuration of operating systems is important to ensuring the reliable operation of computers and the continuous availability and integrity of critical information. Operating systems should be configured so that the security controls throughout the system function effectively and the system can be depended on to support the organization's mission.

Commerce bureaus did not properly configure operating systems to ensure that systems would be available to support bureau missions or prevent the corruption of the information relied on by management and the public. For example, in a large computer system affecting several bureaus, there were thousands of important programs that had not been assigned unique names. In some instances, as many as six different programs all shared the same name,

many of which were different versions of the same program. Although typically the complexity of such a system may require the installation of some programs that are identically named and authorized programs must be able to bypass security in order to operate, there were an excessive number of such programs installed on this system, many of which were capable of bypassing security controls. Because these different programs are identically named, unintended programs could be inadvertently run, potentially resulting in the corruption of data or disruption of system operations. Also, because these powerful programs are duplicated, there is an increased likelihood that they could be misused to bypass security controls.

In this same system, critical parts of the operating system were shared by the test and production systems used to process U.S. export information. Because critical parts were shared, as changes are made in the test system, these changes could also affect the production system. Consequently, changes could be made in the test system that would cause the production system to stop operating normally and shut down. Changes in the test system could also cause important Commerce data in the production system to become corrupted. Commerce management acknowledged that the isolation between these two systems needed to be strengthened to mitigate these risks.

Systems Had Unnecessary and Poorly Configured Functions

Operating system functions should be limited to support only the capabilities needed by each specific computer system. Moreover, these functions should be appropriately configured. Unnecessary operating system functions can be used to gain unauthorized access to a system and target that system for a denial-of-service attack.[22] Poorly configured operating system functions can allow individuals to bypass security controls and access sensitive information without requiring proper identification and authentication.

Unnecessary and poorly configured system functions existed on important computer systems in all the bureaus we reviewed.[23] For example, unnecessary functions allowed us to gain access to a system from the Internet. Through such access and other identified weaknesses, we were able to gain system administration privileges on that system and subsequently gain access to other systems within other Commerce bureaus. Also, poorly configured functions would have allowed users to bypass security controls and gain unrestricted access to all programs and data.

[22] A denial-of-service attack is an attack in which one user takes up so much of a shared resource that none of the resources is left for other users. Denial-of-service attacks compromise the availability of the resources. There are two types of denial-of-service attacks. The first type of attack attempts to damage or destroy resources so you cannot use them. The second type of attack overloads some system service or exhausts some resource, thus preventing others from using that service.

[23] Because of the sensitivity of this information, specific vulnerabilities are not discussed in this testimony. However, the report designated for "Limited Official Use" will describe in more detail the vulnerable functions we identified and offer specific recommendations for correcting them.

Network Security Was Ineffective

Networks are a series of interconnected information technology devices and software that allow groups of individuals to share data, printers, communications systems, electronic mail, and other resources. They provide the entry point for access to electronic information assets and provide users with access to the information technologies they need to satisfy the organization's mission. Controls should restrict access to networks from sources external to the network. Controls should also limit the use of systems from sources internal to the network to authorized users for authorized purposes.

External threats include individuals outside an organization attempting to gain unauthorized access to an organization's networks using the Internet, other networks, or dial-up modems. Another form of external threat is flooding a network with large volumes of access requests so that the network is unable to respond to legitimate requests, one type of denial-of-service attack. External threats can be countered by implementing security controls on the perimeters of the network, such as firewalls,[24] that limit user access and data interchange between systems and users within the organization's network and systems and

[24] Firewalls are hardware and software components that protect one set of system resources (e.g., computers and networks) from attack by outside network users (e.g., Internet users) by blocking and checking all incoming network traffic. Firewalls permit authorized users to access and transmit privileged information and deny access to unauthorized users.

users outside the network, especially on the Internet. An example of perimeter defenses is only allowing pre-approved computer systems from outside the network to exchange certain types of data with computer systems inside the network. External network controls should guard the perimeter of the network from connections with other systems and access by individuals who are not authorized to connect with and use the network.

Internal threats come from sources that are within an organization's networks, such as a disgruntled employee with access privileges who attempts to perform unauthorized activities. Also, an intruder who has successfully penetrated a network's perimeter defenses becomes an internal threat when the intruder attempts to compromise other parts of an organization's network security as a result of gaining access to one system within the network. For example, at Commerce, users of one bureau who have no business need to access export license information on another bureau's network should not have had network connections to that system. External network security controls should prevent unauthorized access from outside threats, but if those controls fail, internal network security controls should also prevent the intruder from gaining unauthorized access to other computer systems within the network.

None of the Commerce bureaus reviewed had effective external and internal network security controls. Individuals, both within and outside Commerce,

could compromise external and internal security controls to gain extensive unauthorized access to Commerce networks and systems. Bureaus employed a series of external control devices, such as firewalls, in some, but not all, of the access paths to their networks. However, these controls did not effectively prevent unauthorized access to Commerce networks from the Internet or through poorly controlled dial-up modems that bypass external controls. For example, four bureaus had not configured their firewalls to adequately protect their information systems from intruders on the Internet. Also, six dial-up modems were installed so that anyone could connect to their network without having to use a password, thereby circumventing the security controls provided by existing firewalls.

Our testing demonstrated that, once access was gained by an unauthorized user on the Internet or through a dial-up modem to one bureau's networks, that intruder could circumvent ineffective internal network controls to gain unauthorized access to other networks within Commerce. Such weak internal network controls could allow an unauthorized intruder or authorized user on one bureau's network to change the configuration of other bureaus' network controls so that the user could observe network traffic, including passwords and sensitive information that Commerce transmits in readable clear text, and disrupt network operations.

The external and internal security controls of the different Commerce bureau networks did not provide a consistent level of security in part because bureaus independently configured and operated their networks as their own individual networks. For example, four of the bureaus we reviewed had their own independently controlled access points to the Internet.

Because the different bureaus' networks are actually logically interconnected and perform as one large interconnected network, the ineffective network security controls of one bureau jeopardize the security of other bureaus' networks. Weaknesses in the external and internal network controls of the individual bureaus heighten the risk that outside intruders with no prior knowledge of bureau user IDs or passwords, as well as Commerce employees with malicious intent, could exploit the other security weaknesses in access and operating system controls discussed above to misuse, improperly disclose, or destroy sensitive information.

Other Information System Controls Were Not Adequate

In addition to logical access controls, other important controls should be in place to ensure the confidentiality, integrity, and reliability of an organization's data. These information system controls include policies, procedures, and techniques to provide appropriate segregation of duties among computer personnel, prevent unauthorized changes to application programs, and ensure

the continuation of computer processing operations in case of unexpected interruption. The Commerce bureaus had weaknesses in each of these areas that heightened the risks already created by their lack of effective access controls.

Computer Duties Were Not Properly Segregated

A fundamental technique for safeguarding programs and data is to segregate the duties and responsibilities of computer personnel to reduce the risk that errors or fraud will occur and go undetected. OMB A-130, Appendix III, requires that roles and responsibilities be divided so that a single individual cannot subvert a critical process. Once policies and job descriptions that support the principles of segregation of duties have been established, access controls can then be implemented to ensure that employees perform only compatible functions.

None of the seven bureaus in our review had specific policies documented to identify and segregate incompatible duties, and bureaus had assigned incompatible duties to staff. For example, staff were performing incompatible computer operations and security duties. In another instance, the bureau's security officer had the dual role of also being the bureau's network administrator. These two functions are not compatible since the individual's familiarity with system security could then allow him or her to bypass security controls either to facilitate performing administrative duties or for malicious purposes.

Furthermore, none of the bureaus reviewed had implemented processes and procedures to mitigate the increased risks of personnel with incompatible duties. Specifically, none of the bureaus had a monitoring process to ensure appropriate segregation of duties, and management did not review access activity. Until Commerce restricts individuals from performing incompatible duties and implements compensating access controls, such as supervision and review, Commerce's sensitive information will face increased risks of improper disclosure, inadvertent or deliberate misuse, and deletion, all of which could occur without detection.

Software Changes Were Not Adequately Controlled

Also important for an organization's information security is ensuring that only authorized and fully tested software is placed in operation. To make certain that software changes are needed, work as intended, and do not result in the loss of data and program integrity, such changes should be documented, authorized, tested, and independently reviewed. Federal guidelines emphasize the importance of establishing controls to monitor the installation of and changes to software to ensure that software functions as expected and that a historical record is maintained of all changes.[23]

[23] NIST Special Publication 800-18: *Guide for Developing Security Plans for Information Technology Systems*, December 1998.

We have previously reported on Commerce's lack of policies on software change controls.[36] Specific key controls not addressed were (1) operating system software changes, monitoring, and access and (2) controls over application software libraries including access to code, movement of software programs, and inventories of software. Moreover, implementation was delegated to the individual bureaus, which had not established written policies or procedures for managing software changes.

Only three of the seven bureaus we reviewed mentioned software change controls in their system security plans, while none of the bureaus had policies or procedures for controlling the installation of software. Such policies are important in order to ensure that software changes do not adversely affect operations or the integrity of the data on the system. Without proper software change controls, there are risks that security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

Service Continuity Planning Was Incomplete

Organizations must take steps to ensure that they are adequately prepared to cope with a loss of operational capability due to earthquakes, fires, sabotage, or other disruptions. An essential element in preparing for such catastrophes is an

[36] *Software Change Controls at Commerce* (GAO/AIMD-00-187R, June 30, 2000).

up-to-date, detailed, and fully tested recovery plan that covers all key computer operations. Such a plan is critical for helping to ensure that information system operations and data can be promptly restored in the event of a service disruption. OMB Circular A-130, Appendix III, requires that agency security plans assure that there is an ability to restore service sufficient to meet the minimal needs of users. Commerce policy also requires a backup or alternate operations strategy.

The Commerce bureaus we reviewed had not developed comprehensive plans to ensure the continuity of service in the event of a service disruption. Described below are examples of service continuity weaknesses we identified at the seven Commerce bureaus.

- None of the seven bureaus had completed recovery plans for all of their sensitive systems.
- Although one bureau had developed two recovery plans, one for its data center and another for its software development installation center, the bureau did not have plans to cover disruptions to the rest of its critical systems, including its local area network.
- Systems at six of the seven bureaus did not have documented backup procedures.

- One bureau stated that it had an agreement with another Commerce bureau to back it up in case of disruptions; however, this agreement had not been documented.
- One bureau stated in its backup strategy that tapes used for system recovery are neither stored off-site nor protected from destruction. For example, backup for its network file servers is kept in a file cabinet in a bureau official's supply room, and backup tapes for a database and web server are kept on the shelf above the server. In case of a destructive event, the backups could be subject to the same damage as the primary files.
- Two bureaus had no backup facilities for key network devices such as firewalls.

Until each of the Commerce bureaus develops and fully tests comprehensive recovery plans for all of its sensitive systems, there is little assurance that in the event of service interruptions, many functions of the organization will not effectively cease and critical data will be lost.

Poor Incident Detection and Response Capabilities Further Impair Security

As our government becomes increasingly dependent on information systems to support sensitive data and mission critical operations, it is essential that agencies protect these resources from misuse and disruption. An important component of such protective efforts is the capability to promptly identify and

respond to incidents of attempted system intrusions. Agencies can better protect their information systems from intruders by developing formalized mechanisms that integrate incident handling functions with the rest of the organizational security infrastructure. Through such mechanisms, agencies can address how to (1) prevent intrusions before they occur, (2) detect intrusions as they occur, (3) respond to successful intrusions, and (4) report intrusions to staff and management.

Although essential to protecting resources, Commerce bureau incident handling capabilities are inadequate in preventing, detecting, responding to, and reporting incidents. Because the bureaus have not implemented comprehensive and consistent incident handling capabilities, decision-making may be haphazard when a suspected incident is detected, thereby impairing responses and reporting. Thus, there is little assurance that unauthorized attempts to access sensitive information will be identified and appropriate actions taken in time to prevent or minimize damage. Until adequate incident detection and response capabilities are established, there is a greater risk that intruders could be successful in copying, modifying, or deleting sensitive data and disrupting essential operations.

Incident Handling Mechanisms Have Not Been Established or Implemented

Accounting for and analyzing computer security incidents are effective ways for organizations to better understand threats to their information systems. Such analyses can also pinpoint vulnerabilities that need to be addressed so that they will not be exploited again. OMB Circular A-130, Appendix III, requires agencies to establish formal incident response mechanisms dedicated to evaluating and responding to security incidents in a manner that protects their own information and helps to protect the information of others who might be affected by the incident. These formal incident response mechanisms should also share information concerning common vulnerabilities and threats within the organization as well as with other organizations. By establishing such mechanisms, agencies help to ensure that they can more effectively coordinate their activities when incidents occur.

Although the Commerce CIO issued a July 1999 memorandum to all bureau CIOs outlining how to prevent, detect, respond to, and report incidents, the guidance has been inconsistently implemented. Six of the seven bureaus we reviewed have only ad hoc processes and procedures for handling incidents. None have established and implemented all of the requirements of the memo. Furthermore, Commerce does not have a centralized function to coordinate the handling of incidents on a departmentwide basis.

Incidents Could Be Prevented

Two preventive measures for deterring system intrusions are to install (1) software updates to correct known vulnerabilities and (2) messages warning intruders that their activities are punishable by law. First, federal guidance, industry advisories, and best practices all stress the importance of installing updated versions of operating system and the software that supports system operations to protect against vulnerabilities that have been discovered in previously released versions. If new versions have not yet been released, "patches" that fix known flaws are often readily available and should be installed in the interim. Updating operating systems and other software to correct these vulnerabilities is important because once vulnerabilities are discovered, technically sophisticated hackers write scripts to exploit them and often post these scripts to the Internet for the widespread use of lesser skilled hackers. Since these scripts are easy to use, many security breaches happen when intruders take advantage of vulnerabilities for which patches are available but system administrators have not applied the patches. Second, Public Law 99-74 requires that a warning message be displayed upon access to all federal computer systems notifying users that unauthorized use is punishable by fines and imprisonment. Not only does the absence of a warning message fail to deter potential intruders, but, according to the law, pursuing and prosecuting intruders is more difficult if they have not been previously made fully aware of the consequences of their actions.

Commerce has not fully instituted these two key measures to prevent incidents. First, many bureau systems do not have system software that has been updated to address known security exposures. For example, during our review, we discovered 20 systems with known vulnerabilities for which patches were available but not installed. Moreover, all the bureaus we reviewed were still running older versions software used on critical control devices that manage network connections. Newer versions of software are available that correct the known security flaws of the versions that were installed. Second, in performing our testing of network security, we observed that warning messages had not been installed for several network paths into Commerce systems that we tested.

Incident Detection Capabilities Have Not Been Implemented

Even though strong controls may not block all intrusions, organizations can reduce the risks associated with such events if they take steps to detect intrusions and the consequent misuse before significant damage can be done. Federal guidance emphasizes the importance of using detection systems to protect systems from the threats associated with increasing network connectivity and reliance on information systems. Additionally, federally funded activities, such as CERT/CC, the Department of Energy's Computer Incident Advisory Capability, and FedCIRC are available to assist organizations in detecting and responding to incidents.

Although the CIO's July memo directs Commerce bureaus to monitor their information systems to detect unusual or suspicious activities, all the bureaus we reviewed were either not using monitoring programs or had only partially implemented their capabilities. For example, only two of the bureaus had installed intrusion detection systems. Also, system and network logs frequently had not been activated or were not reviewed to detect possible unauthorized activity. Moreover, modifications to critical operating system components were not logged, and security reports detailing access to sensitive data and resources were not sent to data owners for their review.

The fact that bureaus we reviewed detected our activities only four times during the 2 months that we performed extensive external testing of Commerce networks, which included probing over 1,000 system devices, indicates that, for the most part, they are unaware of intrusions. For example, although we spent several weeks probing one bureau's networks and obtained access to many of its systems, our activities were never detected. Moreover, during testing we identified evidence of hacker activity that Commerce had not previously detected. Without monitoring their information systems, the bureaus cannot

- know how, when, and who performs specific computer activities,
- be aware of repeated attempts to bypass security, or

- detect suspicious patterns of behavior such as two users with the same ID and password logged on simultaneously or users with system administrator privileges logged on at an unexpected time of the day or night.

As a result, the bureaus have little assurance that potential intrusions will be detected in time to prevent or, at least, minimize damage.

Incident Response Procedures Have Not Been Established

The CIO's July memo also outlines how the bureaus are to respond to detected incidents. Instructions include responses such as notifying appropriate officials, deploying an on-site team to survey the situation, and isolating the attack to learn how it was executed.

Only one of the seven bureaus reviewed has documented response procedures. Consequently, we experienced inconsistent responses when our testing was detected. For example, one bureau responded to our scanning of their systems by scanning ours in return.[27] In another bureau, a Commerce employee who detected our testing responded by launching a software attack against our systems. In neither case was bureau management previously consulted or informed of these responses.

[27] Scanning is a favorite approach of computer hackers to discover what computer network services a computer provides so that it can be probed for vulnerabilities.

The lack of documented incident response procedures increases the risk of inappropriate responses. For example, employees could

- take no action,
- take insufficient actions that fail to limit potential damage,
- take overzealous actions that unnecessarily disrupt critical operations, or
- take actions, such as launching a retaliatory attack, that could be considered improper.

Bureaus Have Not Been Reporting Incidents

The CIO's July memo specifically requires bureau employees who suspect an incident or violation to contact their supervisor and the bureau security officer, who should report the incident to the department's information security manager. Reporting detected incidents is important because this information provides valuable input for risk assessments, helps in prioritizing security improvement efforts, and demonstrates trends of threats to an organization as a whole.

The bureaus we reviewed have not been reporting all detected incidents. During our 2-month testing period, 16 incidents were reported by the seven bureaus collectively, 10 of which were generated to report computer viruses. Four of the other six reported incidents related to our testing activities, one of which

was reported after our discovery of evidence of a successful intrusion that Commerce had not previously detected and reported. However, we observed instances of detected incidents that were not reported to bureau security officers or the department's information security manager. For example, the Commerce employees who responded to our testing by targeting our systems in the two instances discussed above did not report either of the two incidents to their own bureau's security officer.

By not reporting incidents, the bureaus lack assurance that identified security problems have been tracked and eliminated and the targeted system restored and validated. Furthermore, information about incidents could be valuable to other bureaus and assist the department as a whole to recognize and secure systems against general patterns of intrusion.

Commerce Does Not Have An Effective Information Security Management Program

The underlying cause for the numerous weaknesses we identified in bureau information system controls is that Commerce does not have an effective departmentwide information security management program in place to ensure that sensitive data and critical operations receive adequate attention and that the appropriate security controls are implemented to protect them. Our study of security management best practices, as summarized in our 1998 *Executive*

Guide,[28] found that leading organizations manage their information security risks through an ongoing cycle of risk management. This management process involves

(1) establishing a centralized management function to coordinate the continuous cycle of activities while providing guidance and oversight for the security of the organization as a whole, (2) identifying and assessing risks to determine what security measures are needed, (3) establishing and implementing policies and procedures that meet those needs,

(4) promoting security awareness so that users understand the risks and the related policies and procedures in place to mitigate those risks, and

(5) instituting an ongoing monitoring program of tests and evaluations to ensure that policies and procedures are appropriate and effective. However, Commerce's information security management program is not effective in any of these key elements.

Centralized Management Is Weak

Establishing a central management function is the starting point of the information security management cycle mentioned above. This function provides knowledge and expertise on information security and coordinates organizationwide security-related activities associated with the other four segments of the risk management cycle. For example, the function researches

[28] *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

potential threats and vulnerabilities, develops and adjusts organizationwide policies and guidance, educates users about current information security risks and the policies in place to mitigate those risks, and provides oversight to review compliance with policies and to test the effectiveness of controls. This central management function is especially important to managing the increased risks associated with a highly connected computing environment. By providing coordination and oversight of information security activities organizationwide, such a function can help ensure that weaknesses in one unit's systems do not place the entire organization's information assets at undue risk.

According to Commerce policy, broad program responsibility for information security throughout the department is assigned to the CIO. Department of Commerce Organization Order 15-23 of July 5, 2000, specifically tasks the CIO with developing and implementing the department's information security program to assure the confidentiality, integrity, and availability of information and IT resources. These responsibilities include developing policies, procedures, and directives for information security; providing mandatory periodic training in computer security awareness and accepted practice; and identifying and developing security plans for Commerce systems that contain sensitive information. Furthermore, the CIO is also formally charged with carrying out the Secretary's responsibilities for computer security under OMB

Circular A-130, Appendix III for all Commerce bureaus and the Office of the Secretary.

An information security manager under the direction of the Office of the CIO is tasked with carrying out the responsibilities of the security program. These responsibilities, which are clearly defined in department policy, include developing security policies, procedures, and guidance and assuring security oversight through reviews, which include tracking the implementation of required security controls.

Commerce lacks an effective centralized function to facilitate the integrated management of the security of its information system infrastructure. At the time of our review, the CIO, who had no specific budget to fulfill security responsibilities and exercised no direct control over the IT budgets of the Commerce bureaus, stated that he believed that he did not have sufficient resources or the authority to implement the department information security program. Until February 2000, when additional staff positions were established to support the information security manager's responsibilities, the information security manager had no staff to discharge these tasks. As of April 2001, the information security program was supported by a staff of three.

Commerce policy also requires each of its bureaus to implement an information security program that includes a full range of security responsibilities. These

include appointing a bureauwide information security officer as well as security officers for each of the bureau's systems.

However, the Commerce bureaus we reviewed also lack their own centralized functions to coordinate bureau security programs with departmental policies and procedures and to implement effective programs for the security of the bureaus' information systems infrastructure. For example, four bureaus had staff assigned to security roles on a part-time basis and whose security responsibilities were treated as collateral duties.

In view of the widespread interconnectivity of Commerce's systems, the lack of a centralized approach to the management of security is particularly risky since there is no coordinated effort to ensure that minimal security controls are implemented and effective across the department. As demonstrated by our testing, intruders who succeeded in gaining access to a system in a bureau with weak network security could then circumvent the stronger network security of other bureaus. It is, therefore, unlikely that the security posture of the department as a whole will significantly improve until a more integrated security management approach is adopted and sufficient resources allotted to implement and enforce essential security measures departmentwide.

Risks Are Not Assessed

As outlined in our 1998 Executive Guide, understanding the risks associated with information security is the second key element of the information security management cycle. Identifying and assessing information security risks helps to determine what controls are needed and what level of resources should be expended on controls. Federal guidance requires all federal agencies to develop comprehensive information security programs based on assessing and managing risks.[29] Commerce policy regarding information security requires (1) all bureaus to establish and implement a risk management process for all IT resources and (2) system owners to conduct a periodic risk analysis for all sensitive systems within each bureau.

Commerce bureaus we reviewed are not conducting risk assessments for their sensitive systems as required. Only 3 of the bureaus' 94 systems we reviewed[30] had documented risk assessments, one of which was still in draft. Consequently, most of the bureaus' systems are being operated without consideration of the risks associated with their immediate environment.

[29] The February 1996 revision to OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, requires agencies to use a risk-based approach to determine adequate security, including 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 NIST publications and in our *Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33).

[30] For purposes of reviewing Commerce's information management security program, we identified these 94 sensitive systems in the seven bureaus based on our discussions with bureau officials. We also included systems from an inventory of the bureaus' most critical systems that had been prepared by a contractor as part of an assessment of Commerce's Critical Infrastructure Protection Plan as well as from an inventory of critical systems compiled by the department in preparing for their Y2K remediation efforts.

Moreover, these bureaus are not considering risks outside their immediate environment that affect the security of their systems, such as network interconnections with other systems. Although OMB Circular A-130, Appendix III, specifically requires that the risks of connecting to other systems be considered prior to doing so, several bureau officials acknowledged that they had not considered how vulnerabilities in systems that interconnected with theirs could undermine the security of their own systems. Rather, the initial decision to interconnect should have been made by management based on an assessment of the risk involved, the controls in place to mitigate the risk, and the predetermined acceptable level of risk. The widespread lack of risk assessments, as evidenced by the serious access control weaknesses revealed during our testing, indicates that Commerce is doing little to understand and manage risks to its systems.

Security Plans Are Not Prepared

Once risks have been assessed, OMB Circular A-130, Appendix III, requires agencies to document plans to mitigate these risks through system security plans. These plans should contain an overview of a system's security requirements; describe the technical controls planned or in place for meeting those requirements; include rules that delineate the responsibilities of managers and individuals who access the system; and outline training needs, personnel controls, and continuity plans. In summary, security plans should be updated

regularly to reflect significant changes to the system as well as the rapidly changing technical environment and document that all aspects of security for a system have been fully considered, including management, technical, and operational controls.

None of the bureaus we reviewed had security plans for all of their sensitive systems. Of the 94 sensitive systems we reviewed, 87 had no security plans. Of the seven systems that did have security plans, none had been approved by management. Moreover, five of these seven plans did not include all the elements required by OMB Circular A-130, Appendix III. Without comprehensive security plans, the bureaus have no assurance that all aspects of security have been considered in determining the security requirements of the system and that adequate protection has been provided to meet those requirements.

Systems Are Not Authorized

OMB also requires management officials to formally authorize the use of a system before it becomes operational, when a significant change occurs, and at least every 3 years thereafter.[31] Authorization provides quality control in that it forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By

formally authorizing a system for operational use, a manager accepts responsibility for the risks associated with it. Since the security plan establishes the system protection requirements and documents the security controls in place, it should form the basis for management's decision to authorize processing.

As of March 2001, Commerce management had not authorized any of the 94 sensitive systems that we identified. According to the more comprehensive data collected by the Office of the CIO in March 2000, 92 percent of all the department's sensitive systems had not been formally authorized. The lack of authorization indicates that systems' managers had not reviewed and accepted responsibility for the adequacy of the security controls implemented on their systems. As a result, Commerce has no assurance that these systems are being adequately protected.

Needed Policies Have Not Been Established

The third key element of computer security management, as identified during our study of information security management practices at leading organizations, is establishing and implementing policies. Security policies are important because they are the primary mechanism by which management communicates its goals and requirements. Federal guidelines require agencies

[31] Authorization is sometimes referred to as "accreditation."

to frequently update their information security policies in order to assess and counter rapidly evolving threats and vulnerabilities.

Commerce's information security policies are significantly outdated and incomplete. Developed in 1993 and partially revised in 1995, the department's information security policies and procedures manual, *Information Technology Management Handbook,* Chapter 10, "Information Technology Security," and attachment, "Information Technology Security" does not comply with OMB's February 1996 revision to Circular A-130, Appendix III, and does not incorporate more recent NIST guidelines. For example, Commerce's information security policy does not reflect current federal requirements for managing computer security risk on a continuing basis, authorizing processing, providing security awareness training, or performing system reviews. Moreover, because the policy was written before the explosive growth of the Internet and Commerce's extensive use of it, policies related to the risks of current Internet usage are omitted. For example, Commerce has no departmentwide security policies on World Wide Web sites, e-mail, or networking.

Further, Commerce has no departmental policies establishing baseline security requirements for all systems. For example, there is no departmental policy specifying required attributes for passwords, such as minimum length and the

inclusion of special characters. Consequently, security settings differ both among bureaus and from system to system within the same bureau. Furthermore, Commerce lacks consistent policies establishing a standard minimum set of access controls. Having these baseline agencywide policies could eliminate many of the vulnerabilities discovered by our testing, such as configurations that provided users with excessive access to critical system files and sensitive data and expose excessive system information, all of which facilitate intrusions.

The Director of the Office of Information Policy, Planning, and Review and the Information Security Manager stated that Commerce management recognizes the need to update the department information security policy and will begin updating the security sections of the *Information Technology Management Handbook* in the immediate future.

Security Awareness and Training Are Not Adequately Promoted

The fourth key element of the security management cycle involves promoting awareness and conducting required training so that users understand the risks and the related policies and controls in place to mitigate them. Computer intrusions and security breakdowns often occur because computer users fail to take appropriate security measures. For this reason, it is vital that employees who use computer systems in their day-to-day operations are aware of the importance and sensitivity of the information they handle, as well as the

business and legal reasons for maintaining its confidentiality, integrity, and availability.

OMB Circular A-130, Appendix III, requires that employees be trained on how to fulfill their security responsibilities before being allowed access to sensitive systems. The Computer Security Act mandates that all federal employees and contractors who are involved with the management, use, or operation of federal computer systems be provided periodic training in information security awareness and accepted information security practice. Specific training requirements are outlined in NIST guidelines,[32] which establish a mandatory baseline of training in security concepts and procedures and define additional structured training requirements for personnel with security-sensitive responsibilities.

Overall, none of the seven bureaus had documented computer security training procedures and only one of the bureaus had documented its policy for such training. This bureau also used a network user responsibility agreement, which requires that all network users read and sign a one-page agreement describing the network rules. Officials at another bureau stated that they were developing a security awareness policy document.

[32] *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (NIST Special Publication 800-16, April 1998).

Although each of the seven bureaus had informal programs in place, such as a brief overview as part of the one-time general security orientation for new employees, these programs do not meet the requirements of OMB, the Computer Security Act, or NIST Special Publication 800-16. Such brief overviews do not ensure that security risks and responsibilities are understood by all managers, users, and system administrators and operators. Shortcomings in the bureaus' security awareness and training activities are illustrated by the following examples.

- Officials at one bureau told us that they did not see training as an integral part of its security program, and provided an instructional handbook only to users of a specific bureau application.
- Another bureau used a generic computer-based training course distributed by the Department of Defense that described general computer security concepts but was not specific to Commerce's computing environment. Also, this bureau did not maintain records to document who had participated.
- Another bureau had limited awareness practices in place such as distribution of a newsletter to staff, but had no regular training program. Officials at this bureau told us that they were in the process of assessing its training requirements.

Only one Commerce bureau that we reviewed provided periodic refresher training. In addition, staff directly responsible for information security do not receive more extensive training than overviews since security is not considered to be a full-time function requiring special skills and knowledge. Several of the computer security weaknesses we discuss in this testimony indicate that Commerce employees are either unaware of or insensitive to the need for important information system controls.

Policies and Controls Are Not Monitored

The final key element of the security management cycle is an ongoing program of tests and evaluations to ensure that systems are in compliance with policies and that policies and controls are both appropriate and effective. This type of oversight is a fundamental element because it demonstrates management's commitment to the security program, reminds employees of their roles and responsibilities, and identifies and corrects areas of noncompliance and ineffectiveness. For these reasons, OMB Circular A-130, Appendix III, directs that the security controls of major information systems be independently reviewed or audited at least every 3 years. Commerce policy also requires information security program oversight and tasks the program manager with performing compliance reviews of the bureaus as well as verification reviews of individual systems. The government information security reform provisions of

the fiscal year 2001 National Defense Authorization Act require annual independent reviews of IT security in fiscal years 2001 and 2002.

No oversight reviews of the Commerce bureaus' systems have been performed by the staff of Commerce's departmentwide information security program. The information security manager stated that he was not given the resources to perform these functions. Furthermore, the bureaus we reviewed do not monitor the effectiveness of their information security. Only one of the bureaus has performed isolated tests of its systems. In lieu of independent reviews, in May 2000, the Office of the CIO, using a draft of the CIO Council's Security Assessment Framework, requested that all Commerce bureaus submit a self-assessment of the security of their systems based on the existence of risk assessments, security plans, system authorizations, awareness and training programs, service continuity plans, and incident response capabilities. This self-assessment did not require testing or evaluating whether systems were in compliance with policies or the effectiveness of implemented controls. Nevertheless, the Office of the CIO's analysis of the self-assessments showed that 92 percent of Commerce's sensitive systems did not comply with federal security requirements. Specifically, 63 percent of Commerce's systems did not have security plans that comply with federal guidelines, 73 percent had no risk assessments, 64 percent did not have recovery plans, and 92 percent had not been authorized for operational use.

The information security manager further stated that, because of the continued lack of resources, the Office of the CIO would not be able to test and evaluate the effectiveness of Commerce's information security controls to comply with the government information security reform provisions requirement of the fiscal year 2001 National Defense Authorization Act. Instead, the information security manager stated that he would again ask the bureaus to do another self-assessment and would analyze the results. In future years, the information security manager intends to perform hands-on reviews as resources permit.

****

In conclusion, Mr. Chairman, the significant and pervasive weaknesses that we discovered in the seven Commerce bureaus we tested place the data and operations of these bureaus at serious risk. Sensitive economic, personnel, financial, and business confidential information are exposed, allowing potential intruders to read, copy, modify, or delete these data. Moreover, critical operations could effectively cease in the event of accidental or malicious service disruptions.

Poor detection and response capabilities exacerbate the bureaus' vulnerability to intrusions. As demonstrated during our own testing, the bureaus' general inability to notice our activities increases the likelihood that intrusions will not be detected in time to prevent or minimize damage.

These weaknesses are attributable to the lack of an effective information security program, that is, lack of centralized management, a risk-based approach, up-to-date security policies, security awareness and training, and continuous monitoring of the bureaus' compliance with established policies and the effectiveness of implemented controls. These weaknesses are exacerbated by Commerce's highly interconnected computing environment in which the vulnerabilities of individual systems affect the security of systems in the entire department, since a compromise in a single poorly secured system can undermine the security of the multiple systems that connect to it.

To address these weaknesses, we are recommending that the Secretary

- direct the Office of the CIO and the bureaus to develop and implement an action plan for strengthening access controls for Commerce's systems commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or modification of information resulting from unauthorized access. Specifically, this action plan should address the logical access control weaknesses and other information system weaknesses that are summarized in our draft report,
- direct the Office of the CIO to establish a departmentwide incident handling function with formal procedures for preparing for, detecting, responding to, and reporting incidents, and

- direct the Office of the CIO to develop and implement an effective departmentwide security program. Such a program should include establishing a central information security function to manage an ongoing cycle of the following security activities:
  - assessing risks and evaluating needs,
  - updating the information security program policies,
  - developing and implementing a computer security awareness and training program, and
  - developing and implementing a management oversight process that includes periodic compliance reviews and tests of the effectiveness of implemented controls.

We also recommend that the Secretary of Commerce, the Office of the CIO, and the bureau CIOs direct the appropriate resources and authority to fulfill the security responsibilities that Commerce policy and directives task them with performing and to implement these recommendations.

We also recommend that the Secretary take advantage of the opportunity that the installation of the new network infrastructure will provide to improve security.

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

Contacts and Acknowledgments

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

(310125)

U.S. DEPARTMENT OF COMMERCE
Office of Inspector General

BUREAU OF EXPORT ADMINISTRATION

Improvements Are Needed to Meet the Export Licensing Requirements of the 21st Century

Final Inspection Report No. IPE-11488/June 1999

PUBLIC RELEASE

Office of Inspections and Program Evaluations

UNITED STATES DEPARTMENT OF COMMERCE
The Inspector General
Washington, D.C. 20230

June 18, 1999

MEMORANDUM FOR: William A. Reinsch
Under Secretary for Export Administration

FROM: Johnnie E. Frazier
Acting Inspector General

SUBJECT: Final Report: *Improvements Are Needed to Meet the Export Licensing Requirements of the 21st Century* (IPE-11488)

As a follow-up to our May 7, 1999, draft report, this is our final report on our program evaluation of BXA's export licensing efforts. The report includes comments from your June 3, 1999, written response. A copy of your response is included in its entirety as an attachment to the report.

While our report highlights some areas that are working well in BXA, it also highlights problems that hamper BXA's efforts to effectively and efficiently carry out its export licensing responsibilities. The report offers a number of specific recommendations that we believe, if implemented, will better prepare BXA for the export licensing requirements of the 21st century.

Please provide your action plan addressing the recommendations in our report within 60 calendar days. If you have any questions or comments about our report or the requested action plan, please contact me on (202) 482-4661.

We want to thank your entire staff for their assistance and courtesies extended to us during our review.

Attachment

cc: William M. Daley, Secretary of Commerce

unclassified replacement system for ECASS–the analysis did *not* include a classified system alternative.

Both BXA systems personnel and BXA's contractor have confirmed this. Furthermore, we do not believe that BXA's plans to encrypt its new system will address our recommendation for BXA to review the costs and benefits of a classified system. As a result, we strongly reaffirm our recommendation that BXA prepare a cost benefit analysis of implementing a classified database as a part of its new system development effort.

C. ECASS internal controls are generally satisfactory, but some improvements are needed

According to General Accounting Office guidelines, when computer-processed data is an important or integral part of a review and the data's reliability is key to accomplishing the review objectives, reviewers need to satisfy themselves that the data is relevant and reliable.[81] To determine data reliability, the reviewers may either conduct a review of the general and application controls in the computer-based systems, including tests as warranted, or conduct other tests and procedures if the general and application controls are not reviewed or are determined to be unreliable.[82] Since database controls are organized by database operational activity, such as data management, database management, database integrity, database operations, and database security, we identified and tested ECASS general and application controls in those areas. Overall, we determined that ECASS general and application controls are generally adequate and that ECASS data are sufficiently reliable but some controls need strengthening or further implementation.

BXA has adequate data management controls in place

Data management addresses how data is defined, input, and controlled usually through an active data dictionary and database administrator.[83] Without adequate data management, data elements are not controlled, incorrect data may be placed into production, and standard data definitions are not enforced. We found that the ECASS data elements are well defined and controlled. We also found that the data management function has sufficient organizational authority and is properly divided between administrative and technical functions, and the data audit trail is fairly complete. However, we determined that the audit trail can be improved, documenting changes to

---

[81] *Assessing the Reliability of Computer-Processed Data,* General Accounting Office, April 1991.

[82] General controls: The structure, methods, and procedures that apply to all computer operations in an agency, including organization and management controls, security controls, and system software and hardware controls. Application controls: Methods and procedures designed for each application to ensure the authority of data origination, accuracy of data input, integrity of processing, and verification and distribution of output.

[83] An active data dictionary provides an online list of standardized file names and ensures that database and data dictionary file names are consistent. Users cannot define or access data unless those data definitions are processed through the data dictionary system.

recommendations in open and closed licenses can be improved, and the ECASS data element responsibility can be assigned to the individuals who use the individual data elements.

Data audit trail complete but needs improvement

Office of Management and Budget Circular A-123 (Revised) states that government agencies must maintain documentation to justify decisions and operations. An audit trail in a database environment comprises data input, processing, and output to substantiate transaction processing, support financial or other critical totals, and provide a means to reconstruct the database in the event of a system crash or major processing problem. The nature of BXA operations, whereby hundreds of users share the same database from on-line terminals through local and wide area networks, magnifies the importance of an adequate system audit trail.

We found that BXA's licensing process provides a fairly complete audit trail to reliably assess licensing performance. This audit trail comprises 11 major elements: (1) paper and automated license applications;[84] (2) automated license applications containing licensing decisions by licensing officers, supervisors, and referral agencies; (3) paper files maintained by licensing officers; (4) paper Operating Committee licensing decisions disseminated to licensing officers and the referral agencies; (5) scanned exporter technical specifications;[85] (6) current and archived licenses in ECASS; (7) backup tapes of current and archived licenses; (8) the ECASS file that documents reopened cases; (9) the ECASS logs that record database and security activities; (10) system documentation for each program change; and (11) ECASS verification of data transmitted to the referral agencies.

Even with these 11 major elements, BXA's system audit trail is systemically limited. ECASS cannot combine key license elements into one automated file; for example, the license application, database updates and modifications, and applicable exporter technical specifications are in separate systems.[86] ECASS has no central repository where a user can go to directly view all database updates and modifications. However, this limitation has not precluded BXA from having an adequate audit trail because the 11 major elements of BXA's audit trail complement one another.

In addition to the above limitation, we identified four areas relating to the audit trail that need correction. First, ECASS does not record what change has been made to each field. The ECASS

---

[84]Exporter paper applications become automated license applications after they are scanned in and verified.

[85]Exporter technical specifications include brochures and design drawings.

[86]The Multipurpose Archival and Records Retrieval System electronically archives all export license documents and forms by scanning paper documents and storing them as images on a server in BXA's network room. The system became operational in fiscal year 1997 to replace BXA's old microfiche system.

electronic record only records when and by whom a change to a data field was made. If, for example, licensing officers make changes to data fields in pending licenses, the current data in that field is "written over," or eliminated. The database management system (or Model 204) cannot "audit" each field in the database to show what specific changes are made. As a result, licensing officers are supposed to "document" changes in licensing officer notes, but that is not consistently done. To determine what fields have been changed, BXA personnel would have to painstakingly compare different versions of backup tapes. To correct this problem, BXA's Acting Chief Information Officer stated that a separate record with the old value will be coded to show the old and new value. We agree that this change will improve the ECASS audit trail. For issued cases, BXA's audit trail comprises an electronic record documenting who, when, and what was changed.

Second, BXA does not ensure that all license conditions agreed to by the Operating Committee are correctly inputted into ECASS. If conditions are not properly input, the audit trail changes, data integrity is affected, and quality control is reduced.

Third, we found that the departmental computer center in Springfield is adequately maintaining automated applications by backing up the ECASS database on a daily, weekly, and monthly basis, and copies are stored at the center and at the Department of Commerce headquarters. However, there is the possibility that these tapes could be modified by BXA personnel, invalidating the audit trail. In 1993 we recommended that BXA provide a duplicate read-only tape to the Under Secretary for Export Administration every day, highlighting any changes that might be made by lower ranking BXA personnel. BXA personnel stated that getting the tape to the Under Secretary's office and finding enough space to store it would be a difficult daily task. As a result, this has not happened. Since we still maintain that the audit trail would be strengthened by having the stored databases owned by BXA's Under Secretary with read-only access to produce historical reports as required, we recommend that a duplicate read-only tape be provided to the Under Secretary every 90 days, highlighting any changes that might be made by lower ranking BXA personnel.

Fourth, we also recommended in the 1993 report that paper applications and technical specifications be retained for five years. Currently, BXA physically retains hard-copy information for only 90 days except memorandums from BXA personnel or exporters requesting system changes, which are maintained for one year. BXA personnel stated that maintaining paper applications for five years is too long. We are satisfied that maintaining paper applications for 90 days is adequate.

Improvements are needed to better document changes to recommendations of open and closed cases in ECASS

We examined ECASS to determine whether recommendations entered into the database were later changed without the consent or knowledge of licensing officials. We found two key controls to preclude this from happening.

The first control is that supervisors cannot make changes to pending or closed licenses without the licensing officers' knowledge.[87] For pending licenses, supervisors can only verbally suggest changes to LOs or insert changes into the licensing officer notes section of the automated license application. For example, supervisors can request that LOs reject licenses based on current intelligence that the LOs are not privy to. If the LOs are verbally instructed to make changes, they are supposed to document the request in the LO notes section. However, we have found that the LOs do not consistently document their changes or changes requested by a supervisor in LO notes. If a supervisor goes into the file and electronically requests that an LO make changes to a pending license, ECASS automatically documents the request. Supervisors can move cases from one LO to another to balance an LO's workload, but again, the supervisors cannot physically make changes in the system. Even cases decided by the Operating Committee and the Advisory Committee on Export Policy are returned to the LOs for inclusion of new conditions and/or deletion of conditions. Our survey confirmed that the LOs believe that their recommendations are not changed without their consent or knowledge.

For closed licenses, supervisors, LOs, and exporters must submit a written request to BXA's operations staff to reopen a case and make the appropriate change. Changes to cases closed and archived are rare, with only 120 cases reopened in fiscal year 1998 (out of approximately 11,000 license applications). After the operations staff reopens a case and makes the appropriate change, the case is then sent to the applicable LO for review. Reasons for reopened cases included: correcting data input errors; changing case decisions from denied to approved or approved with conditions, and adding or deleting conditions as a result of the escalation or appeals processes.

However, we identified two areas where corrections are needed. First, BXA lacks written criteria for when a case can be reopened. Second, although the operations staff receive written justifications for reopening a case, no one periodically reviews the reopened case report to ensure that valid reasons for reopening cases are received and that the electronic audit trail describing why the case was reopened is complete. We found that the electronic audit trail ranged from very complete descriptions of why a case was reopened and who requested the case be reopened, to very minimal descriptions of why a case was reopened (e.g., "modify conditions") and no description of who made the request. This is an important audit trail issue because when the paper document requesting a case be reopened is eliminated, the electronic audit trail is the only source for why a case was reopened. BXA needs to ensure that the electronic audit trail is more complete.

The second control to prevent unauthorized changes to ECASS involved the interagency referral process. We found that Defense, Energy, and the Nonproliferation Center could not make changes either directly to ECASS from their ECASS terminals or to the ECASS files they

[87]Countersigners or supervisors review and sign off on license cases from the licensing officers before the licenses are issued, returned without action, or denied.

download to their systems. We also found that State and ACDA could not make changes directly to ECASS from their ECASS terminals.

ECASS data element responsibility has not been assigned to the individuals who own the individual data elements

Although BXA's operations staff scans and verifies application data before it goes into ECASS, they do not "own" the data. BXA has identified 18 "principles" that its future system will incorporate, the 7th of which states that "The managers of the organizations entering and capturing the data will be accountable for its accuracy and content."[88] Under the proposed new system, BXA senior management must indicate their desire to manage data and, through a database administrator, assign data element responsibilities to individuals throughout the organization. Thus, an individual or individuals would have the responsibility for authorizing access to the data element, and assuring the integrity of the data element.

Database management controls have ensured that ECASS has run properly for many years

Adequate database management requires an appropriate organizational structure and resources needed to effectively use database technology and recognize and prevent risks. ECASS has been well managed for many years by the same individual who ensures that data elements are well defined, analyzes database performance statistics, and corrects problems that occur. However, this individual is a contractor who has never been officially designated as the database administrator. BXA needs to officially designate a database administrator, designate an official database review board, perform ongoing internal control reviews, and reorganize ECASS.

BXA has not officially designated a data base administrator

In 1991, we recommended and BXA agreed to develop a charter that clearly identifies the duties and responsibilities of a database administrator and ensure that a database administrator performs these duties.[89] While BXA had a database administrator for about three years after our review, when he left, BXA did not fill the position. Since then, BXA's de facto database administrator has been a contractor. BXA has not prepared a charter for the de facto database administrator. BXA's Acting Chief Information Officer plans to designate himself the official administrator and prepare a charter. We believe this action will satisfy this requirement.

---

[88] *Task 5: Information Architecture,* Booz Allen & Hamilton, October 1998.

[89] *Inspection of ECASS Internal Controls,* Final Report, Office of Inspector General, June 1991.

BXA lacks an official database review board

BXA needs a review board that is independent of the database administrator and software team to ensure that ECASS database standards and procedures are being followed and that ECASS is meeting user needs. In some organizations, these boards are called quality assurance boards or systems assurance groups and have their own charter. While BXA has an IT Steering Committee, it lacks a charter. In addition, this committee has focused solely on BXA's system re-engineering project and not on database standards and procedures. BXA's contractor recommended that a standards development group be "constituted to establish the appropriate database standards," including data definition, data documentation, passwords, and writing and testing programs.[90] In order for an organization to achieve promised performance, specific standards must be established and plans developed to achieve the standards. This process requires the continual monitoring of results versus standards. Database leaders should work with users to develop performance standards which are then measured against results.

BXA does not perform ongoing internal control reviews

Internal controls must be periodically reviewed to determine whether they are functioning as planned. Although BXA personnel have performed prior internal control reviews of ECASS, the last documented review was performed in 1991. However, ECASS has undergone numerous changes since then. BXA's standards team could perform ongoing internal control reviews, or BXA could establish a team to periodically (about once a year or when conditions materially change) review the internal controls and risks associated with its system. The team could comprise the database administrator, security officer, users, database analysts, and operations personnel.

BXA has not reorganized ECASS in two years

In 1991, we recommended that BXA reorganize and verify the database, using appropriate software, and maintain a record of results. BXA personnel informed us during our current review that the database has been reorganized a few times since 1991, but not since 1997. After normal usage, data becomes physically unorganized, logically unlinked, and possibly lost. The physical and logical database needs to be restructured periodically to meet the changing needs of users. A database verifier is a software package that reviews the integrity of the database to ascertain that all the designated paths through the database are complete. Reorganizing ECASS will arrange files more efficiently and ensure data linkage. BXA's database administrator should reorganize the database every year.

---

[90] *Task 5: Information Architecture,* Booz Allen & Hamilton, October 1998.

Database integrity controls need improvement

Database integrity controls help the database administrator ensure the accuracy, completeness, and authorization of database data. Without adequate database integrity controls, inaccurate or incomplete data can be entered into ECASS, data may not be entered on a timely basis, and integrity errors may not be detected. We evaluated ECASS data input and processing controls to determine data and system integrity, finding that changes to pending, issued, and archived licenses are adequately controlled. However, the overall process of inputting and verifying paper licenses is an ineffective process prone to errors. Data processing controls have allowed some licenses to be issued without exporter codes and export control classification numbers.

Data input controls need improvement

While it is unlikely that any computer system contains error-free data, we found that (1) paper applications take too long to get scanned, verified, and inputted into ECASS, (2) paper applications get scanned, verified, and inputted into ECASS with errors, and (3) some exporters, consignees, and end users have more than one identification number. As mentioned previously, BXA and its system contractor prepared 18 principles for its new information system architecture to ensure data consistency, accuracy, quality, and system integrity.[91] However, until BXA's new system is developed and its 18 principles implemented, the three problems described above need to be addressed and corrected.

First, BXA's License Application Scanning System was implemented in 1994 to process paper license applications using a PC-based forms processing and image management system. We found that, before being loaded into ECASS, scanned applications take too long to process. BXA receives approximately 200 license applications a week. In fiscal year 1998, it took an average of 5.4 days to input each application. BXA personnel stated that scanning and verification have been inadequate because of (1) poor work and low motivation of the employees, (2) poor staff management, (3) increased applications, and (4) the habitual illnesses of some staff members. BXA is currently testing a new system, called SNAP, whereby exporters will submit license applications over the Internet. BXA personnel hope that the electronic submission of licenses will significantly reduce the number of paper applications. If the new system does not successfully reduce paper applications, BXA would like to mandate that all paper applications be replaced by the new system. Although we agree, this might be difficult to enforce. When asked if some type of outreach effort would influence exporters to use the new system, BXA personnel stated that they have been performing outreach efforts.

Second, the licensing officers have complained that the poor quality of some inputted applications causes them to have to make changes or submit changes to the operations staff. Input controls are critical in a database environment because many programs use the same data for processing.

---

[91] *Task 5: Information Architecture,* Booz Allen & Hamilton, October 1998.

Thus, there must be increased reliability. From February 1, 1998, to February 1, 1999, BXA received 7,333 applications and the operations staff made changes to 3,766 of these applications (51 percent). From November 1998 through January 1999, about 45 percent of the applications had at least one change, such as an address change or inputting a missing sentence. BXA personnel cited little quality control of verified applications before they are entered into ECASS as the reason for the number of changes being made by the operations staff and LOs. The operations staff director stated that she believes her staff finds most errors because there were only 120 cases reopened in fiscal year 1998 for various reasons–not just data input errors. However, these changes should be corrected before the applications are inputted into ECASS, because some errors may not be detected by the operations staff, LOs, and outside parties, and remain in the database.

We suggested that BXA consider the feasibility of one clerk's work being reviewed by another before it goes into the database or contract this function out. The operations staff director stated that her staff does not have time for such reviews, nor does BXA have the funding to contract out this function. However, if BXA's new system greatly reduces the number of paper applications, the operations staff should have time for this quality control measure. In addition, BXA personnel suggested that the old "User Meetings" between the operations staff, LOs, and Information Technology staff should be reestablished so that issues are discussed and problems quickly identified and resolved. We concur with that suggestion.

Third, the Office of Export Enforcement uses a computer name-matching program to assign unique identification numbers to all exporters, consignees, and end users on an application, so that its agents can flag and review any party to a case. However, some exporters, consignees, and end users in the ECASS database have more than one identification number, resulting in a long watchlist, lengthy searches for the LOs, and some identification numbers that may not get flagged by the Office of Export Enforcement.

Although data integrity means that the same company does not have more than one identification number, this was not an initial business rule of BXA. For many years, Export Enforcement assigned a different code to an exporter, consignee, or end user even if their name and address was only slightly different. More importantly, Export Enforcement assigned different codes to a company even if that company, with the same name and address, already had an identification number. Export Enforcement did this to ensure that all parties to a case were added to or screened against its watchlist. However, the General Accounting Office stated that BXA has not ensured that each party is given only one identification number and has in some cases assigned multiple identification numbers to the same party.[92] Some of these identification numbers have watchlist flags, while others do not. As a result, license applications involving parties on the watchlist may not be caught because the parties may be assigned identification numbers that do

[92] *Export Controls: License Screening and Compliance Procedures Need Strengthening,* General Accounting Office, NSIAD-94-178, May 1994.

not carry watchlist flags. BXA personnel stated that multiple identification numbers provide the LOs and export enforcement agents with different results when they query ECASS. As a result, both LOs and agents must submit queries many different ways to ensure that they find all relevant information.

By evaluating just one page of BXA's January 1997 Watchlist printout, we found several company entries that were spelled the same and had the same addresses (e.g., OIG Corporation) and companies that were spelled differently (e.g., OIG Corp. or Office of Inspector General Corporation) that had the same and different addresses. All of these entries had different identification numbers. We asked BXA if they could determine how many companies are in the database (i.e., OIG Corporation) but are spelled differently (i.e., Office of Inspector General Corporation, or OIG Corp.). To answer our question, BXA personnel stated that they would have to use many hours of system processing time, which would affect the processing of licenses. BXA's new system is expected to have an improved identification numbering process. In the meantime, BXA personnel stated that companies with duplicate identification numbers remain in the database, which makes reviewing all companies provided by a licensing officer query a very time consuming task.

BXA has taken steps to reduce the number of duplicate codes in its database, including an extensive archiving effort to retire a large number of duplicate company entries. For example, in 1993, BXA evaluated two states and two countries to determine what duplicate companies existed, finding and archiving many of them. However, BXA has not performed a similar review since 1993. This needs to be done.

Coding and case numbering controls need improvement

Although we found that most data processing controls were adequate, a few cases were issued without a code and/or export control classification numbers. We identified five cases that were issued without being properly coded. Specifically, three cases were issued without the end users being coded, and two were issued without the system being set to "Y" (yes) indicating the parties had been coded. We also found that 35 cases were issued without export control classification numbers. According to the General Accounting Office, each computer system should have steps aimed at ensuring the accuracy of computer processing, and these steps are designed to verify that all relevant records were completely processed and, more importantly, that computer processing met the intended objectives of the system.[93]

Although the number of cases issued without codes and numbers is small compared to all the cases in the database, this is still a serious breach of internal controls. BXA personnel could only speculate on why cases had been issued without codes or numbers. At our request, they have agreed to determine what caused this breakdown in data processing controls. Without a code for

[93] *Assessing the Reliability of Computer-Processed Data,* April 1991.

an exporter, consignee, or end user, Export Enforcement cannot perform a match against its watchlist.

Operating Committee Chair does not verify that conditions agreed upon on each case are placed on the final license

According to the Executive Order 12981, the conditions agreed to by the Operating Committee should be the official record. However, as discussed in Section V of this report, we found some issued cases where conditions that exporters must comply with, and agreed to by the Operating Committee, have been changed, which seriously undermines data integrity.

Database operations have been significantly improved

Database operations comprise the day-to-day maintenance and recovery procedures of the database. Since ECASS runs on a mainframe computer at the departmental computer center in Springfield, a large part of database operations is handled by that staff. In February 1998, the Office of Inspector General reviewed the general controls pertaining to the center's management, operations, and security. At that time, we recommended improvements in the center's security program, access control, segregation of duties, system software, and service continuity.[94] During our current review, we found that the center had made significant improvements to access controls, security, and service continuity. Both the center and BXA maintain adequate copies of database information. However, we found that BXA lacks a current contingency plan and risk analysis, and BXA personnel do not know where to report database problems.

BXA lacks a system contingency plan

In 1991, we recommended that BXA revise and test its ECASS disaster plan and train appropriate personnel in its use to comply with Federal Information Processing Standards Publication 87 guidelines.[95] Federal Publication 87 states that unless contingency plans are continually reviewed and tested, they may fail when needed. Personnel should test contingency plans at the designated backup site by taking copies of all needed data and other information. The test should show that the backup site remains unharmed in a simulated catastrophe or disruption or service.

BXA personnel stated that they had taken an old disaster plan and converted it into a current continuity-of-operations plan but the new plan needs improvement. BXA's contractor, as part of a Year 2000 Business Continuity and Contingency Plan for BXA mission critical systems and high

[94] *Office of Computer Services General Controls,* Office of Inspector General, Audit Report No. FSD-10021-8-0001, February 18, 1998.

[95] *ECASS Internal Controls,* June 1991.

priority non-mission critical systems, plans to upgrade its current continuity-of-operations plan to include BXA policy and procedures regarding security of BXA systems, prevention, incident handling, and planned response to catastrophic emergency events.[96] BXA plans to disseminate its plan to all employees.

Although BXA has historically relied on the Springfield Computer Center in the event of a system catastrophe, there are other issues that BXA needs to document including how its network and users would operate after a catastrophe. BXA does not believe that its network warrants a complete backup facility, due to the small probability of a catastrophic network failure. BXA will include its local area network facility in its plan. BXA plans to do export licensing outside of its network via dial-up from LO and special agent workstations. However, we found that BXA lacks written procedures for its LOs and agents to use. Because BXA's core mission of processing licenses depends on the Springfield Computer Center's hot-site contingency plan, if there is a problem at the center, BXA's licensing operation is in jeopardy. The contractor who prepared a draft 2000 Business Continuity and Contingency Plan for BXA recommended that BXA develop, where possible, manual licensing and enforcement contingency processes. We agree that BXA should update its plan to include all appropriate manual and system contingency processes as soon as possible.

BXA lacks a risk analysis/vulnerability assessment

BXA has not updated its risk analysis in five years. Federal Publication 65 states that risk analyses should be conducted at least every three years and when significant changes are made to the equipment, system, or physical environment. A risk analysis should document system vulnerabilities, threats, and safeguards. In addition to having exceeded the three-year standard, BXA is planning to significantly change its system, equipment, and physical environment. Before this is done, BXA needs to update its risk analysis to outline the potential unfavorable events and the corresponding safeguards. For example, moving to a new system at Commerce headquarters could be very disruptive unless BXA has outlined potentially unfavorable events and the corresponding safeguards.

BXA plans to complete a vulnerability assessment of ECASS during fiscal year 1999.[97] To address this issue, BXA should either establish a risk management team to identify and assess the severity of risk in its database environment or have a contractor perform the assessment. A risk management team comprised of users, database analysts, security personnel, and data processing personnel would have detailed knowledge of the system. Although more costly, a contractor would provide an outsider's independent view of the system.

---

[96] *BXA IT Strategic Plan for FY 1999-2004,* January 1999.

[97] *BXA IT Strategic Plan for FY 1999-2004,* January 1999.

BXA personnel do not know where to report database malfunctions

Although BXA's Acting Chief Information Officer stated that BXA personnel are suppose to call the BXA hotline with all problems, we told him that some personnel were unaware of where to call witn a database problem. BXA personnel stated that they would only call the hotline with a problem that directly affected them, such as their computer breaking down. If a larger problem occurred, BXA personnel stated that they would call BXA's main database analyst and lead programmer. Malfunction reporting provides a formal process that normally involves a form and procedures to identify the malfunction, its potential cause, and potential course of action. BXA's database administrator receives daily database error reports, but he has not designed a form for users of the database to complete and return when suspected problems have been detected. A database malfunction reporting process could encourage users to present any condition that may not be a database problem, such as a personal computer not working, as a database problem. However, with BXA planning to implement a new database environment, a malfunction reporting process is needed. BXA needs to send out a "network message" to emphasize that all database problems should be reported via the hotline.

Database security controls have improved, but additional improvements are needed

Database security comprises the overall methods, procedures, and techniques used to prevent, detect, and correct intentional, unintentional, and unauthorized access to the database. By reviewing the general controls, including security controls, of the departmental computer center, we found that access to and use of the ECASS have greatly improved. However, we found that BXA's security controls could be improved by improving database access controls, preparing a security plan, performing periodic security reviews, officially assigning the security duties to its security officer, providing all users with current security training, and restricting the number of BXA employees with file manager access.

BXA lacks a security plan

We found that BXA had no strategic security plan addressing its licensing process. It had no overall strategy to minimize risk and thereby safeguard sensitive license information. According to the Commerce *ADP Security Manual*, effective security planning is the basic prerequisite for implementing any cost-effective system of security controls. It requires (1) the application of risk analysis techniques to improve the security planning process, (2) a continuing evaluation of security measures, and (3) the safeguarding of data processed by a system. BXA's security officer is aware of BXA's need for an overall security plan. She found an old BXA security plan and plans to prepare a new plan. We would like to review BXA's new security plan before it is issued in final.

BXA does not perform periodic security reviews or tests

BXA's security officer could not remember when the last security review of ECASS was conducted. Without routine, repeated reviews, security weaknesses may not be promptly identified or corrected. The Department's *ADP Security Manual* requires continuing security evaluations be performed. We recommend that BXA conduct yearly security reviews to update and improve ECASS security, improve user security awareness, and improve security training. BXA's security officer agrees with our recommendation, stating that she plans to set up a security program including periodic security tests.

BXA has not officially assigned its security responsibilities

BXA's Information Technology Strategic Plan for fiscal years 1999-2004 states that BXA appointed an IT security officer in the latter half of 1998. However, the appointed individual stated that she had not been officially designated the security officer. Specifically, she has not received an official designation in writing or had her performance plan updated to reflect her new duties. We found that some LOs were uninformed of who the BXA security officer was and where to report security incidents. BXA's Security Standards Operating Procedures state that employees should report all suspected or actual security incidents to their supervisor and the ECASS Security Administrator.[98] However, if the LOs do not know who the security administrator is, reporting security incidents is difficult. BXA needs to designate its current security officer as the official security officer and distribute a network message stating who is the security officer and where to report incidents. BXA should also provide the security administrator's telephone number in its security manual.

BXA users, including BXA's security officer, have not received complete security training

BXA's security officer stated that she plans to provide security awareness training to everyone with network access. Some BXA personnel stated that they had not received any security training over the last few years. As a first step, BXA's security officer plans to issue and have all BXA employees sign for BXA's updated security manual. BXA's security officer would also like to attend a training session on ACF-2, which is the security package used by the Springfield Computer Center. She has little knowledge of the capabilities of the package, and what security improvements, if any, could be made.

---

[98] *Security Standard Operating Procedures, Export Control Automated Support System,* Bureau of Export Administration, March 1999.

Database access controls need to be improved

In February 1998, the OIG issued a report documenting the Office of Computer Services general controls.[99] The report stated that the office controls needed improvement in access control. During our current review, we found three problems with access controls identified in our prior report that had not been addressed: (1) the Springfield Computer Center is not regularly analyzing security violations, (2) the center is not analyzing user access privileges, and (3) BXA and the center lack an electronic mechanism where terminated/transferred employees are immediately removed from center access.

Database access controls assure that only authorized individuals gain access to database resources. Feedback information should indicate both the number of times the access rules prevent an unauthorized access, and the number of detected access violations. During our inspection, we found that the center was still not regularly monitoring its security log for security violations. The individual responsible for this activity at the center stated that the center lacked adequate resources to perform this function. We recommended that the Acting Director consider hiring a third individual to assist in performing log-on account administration, to provide existing personnel with more time for such duties as monitoring violation reports. The Acting Director agreed to consider hiring a third individual depending on any reorganization or job function changes. The office needs to start regularly monitoring its security log as soon as possible.

During our inspection, we found that neither BXA nor the center was regularly analyzing the population of inactive log-on accounts and multiple and generic log-on IDs. In our prior report, we recommended that the center analyze the population of inactive log-on accounts in the ACF-2 database and delete and suspend accounts no longer needed, and analyze the population of multiple and generic log-on IDs and delete all unnecessary duplicates.[100] The center's Acting Director stated that the center analyzed the database in November 1997 and suspended all identification numbers that had been inactive for 60 days. He further stated that the center's security team would review the ID database on a quarterly basis, and take appropriate action. However, from November 1997 to March 1999, only one review had been performed. The center needs to perform these analyses every quarter.

BXA is not immediately notifying the center when users move or are terminated. During our prior review, we found that there was no reliable mechanism for informing the center of employee transfers or terminations. Formal procedures and direct communication lines between center personnel and security departments would increase the effectiveness of controlling user access to the production environment. We recommended that the center develop communication links to client personnel departments for immediate notification of terminated or transferring employees in order for system access to be promptly revoked or modified. Center personnel stated that center

[99] *Office of Computer Services General Controls*, February 1998.

[100] *Office of Computer Services General Controls*.

procedures require each client to have a security administrator who is responsible for notifying the center security when an employee is terminated or transferred. However, we recently determined that BXA's security officer had not notified the center of some terminated or transferring employees. Center security will institute a procedure whereby client personnel departments will be queried to ascertain terminated or transferred employees.

We reaffirm our recommendation that a communication link be developed to immediately notify the center of terminated or transferring employees in order for system access to be promptly revoked or modified (by the end of each working day).

Too many BXA IT employees have file manager access

Five BXA employees have file manager access to ECASS. This is too many, since this level of access can override all system controls. File manager access needs to be restricted to only the database administrator and a backup.

In its written response to our draft report, BXA generally agreed with all of our recommendations to implement or strengthen the internal controls for ECASS. With regard to our recommendation to have the database administrator assign data element responsibilities to individuals throughout the organization, BXA stated it plans to assign ownership of data elements to BXA organizations and subunits. We concur with this suggestion. In addition, we recommended that BXA designate an official database review board that is independent of the database administrator, but it responded that these functions should be handled by its Chief Information Officer. We concur with this suggestion.

With regard to our recommendation that BXA determine why some cases were issued without codes or Export Control Classification Numbers, BXA indicated that it has researched this issue and found that it occurred in only a minimal number of cases and it has not occurred at all since 1996. BXA does not believe further attempts will be successful. However, if this happens again, BXA has implemented procedures to quickly determine why such cases have been issued. This action satisfies our recommendation.

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

JUN 13 2001

MEMORANDUM FOR Secretarial Officers
Heads of Operating Units

FROM: Donald L. Evans

SUBJECT: Strengthening Commerce Information Technology Management

In order to manage and be accountable for public assets and to ensure that limited public dollars are being spent for the most critical needs, we must strengthen the management of information technology (IT) in the Department. IT is important to the Department's mission, and IT expenditures represent a significant part of the Department's budget. Effective IT capital investment planning is critical.

Therefore, I request that you implement the Department of Commerce IT Restructuring Plan, a copy of which is attached. Department-wide implementation of this plan will be overseen by the Department's Chief Information Officer.

Attachment

DEPARTMENT OF COMMERCE

Information Technology (IT) Restructuring Plan

In order to strengthen the Department's management of IT:

1. Each operating unit (and major NOAA line offices) will establish a Chief Information Officer, who will report to the head of the operating unit (Under Secretary, Assistant Secretary, Director, or Administrator) or principal Deputy, and to the Departmental CIO.

2. Operating unit CIOs will be responsible for advising the operating unit on all aspects of IT and for developing and recommending policies for managing IT within the operating unit, consistent with Departmental policies and guidelines.

3. Operating unit CIOs will have line authority and responsibility for centralized IT functions. At a minimum, those functions that will be centralized under the CIOs will be:

   a. IT for Office Support
   b. Telecommunications Networks
   c. Administrative Data Centers
   d. Website Support
   e. IT for Forms and Records
   f. IT for Administration, including Human Resources, Purchasing, Security and Facilities Management.

4. The performance plan for each operating unit CIO will be established and evaluated by the Head of the Operating Unit (or that person's designee) in consultation with the Department CIO (or, in the case of NOAA line offices, the NOAA CIO as delegated by the Department CIO).

5. The operating unit CIO will establish and evaluate a critical element of the performance plan for the most senior IT manager for those IT personnel who do not report to the CIO. The intent of this element is to ensure that all IT personnel in an operating unit have in their management chain someone who is responsible to the CIO for improvements in IT management.

6. All employees of the Department who perform IT work will have an element in their performance plan that evaluates their improvement in the way their IT work is performed. This element will be established and evaluated by the employee's direct supervisor. The purpose of this element is to require employees who perform IT work as part of their job (including researchers, economists, etc.) to improve how their IT work is done, similar to the way we have used the "diversity" critical element.

7. The operating unit CIO must concur in the budgeting and expenditure of funds for IT by the operating unit. In the event the operating unit CIO does not concur, the Head of the Operating Unit will be the deciding official. The operating unit CIO will provide guidelines to allow small and routine expenditures to be made without further explicit approval.

8. The Department CIO will report to the Secretary. The performance plans for both the CIO and CFO/ASA will include elements ensuring continued strong cooperation between their offices. The CIO's performance plan will be changed to reflect the increased responsibility and authority due to the reorganization.

9. Within sixty (60) days of the approval of this reorganization, the head of each operating unit will submit a plan for the approval of the Assistant Secretary for Administration and the Department Chief Information Officer detailing how these recommendations will be implemented in the operating unit.

MEMORANDUM FOR Chief Information Officers

FROM: Thomas N. Pyke, Jr.
Acting Chief Information Officer

SUBJECT: Revised Capital Asset Plans

The Office of Management and Budget (OMB) has issued new guidance for preparing and submitting budget estimates. Circular A-11, Preparation and Submission of Budget Estimates, is available at http://www.whitehouse.gov/omb/circulars/a11/01toc.html. Copies of the sections relevant to information technology, specifically Exhibits 300 (Capital Asset Plan and Justification) and 53 (Agency IT Investment Portfolio) and supporting documentation, are attached. A template for the Exhibit 300 is available at http://cio.gov/Documents/exhibit%5F300%5Ftemplate%5F2003%2Edoc.

Exhibit 300 has been modified as follows:

- Exhibits 300A and 300B have been combined to form Exhibit 300.
- Part I, Section A includes additional questions.
- Part I, Section C is a new requirement for a brief project description.
- Part II, Sections B-G include quite a number of changes. Please read and answer all the questions carefully.
    - In section E on Enterprise Architecture, cite the specific sections of your architecture plan that pertain to this investment. A Web link would be helpful.
    - Section F on Security and Privacy is a particular focus this year. Take care to answer all the questions thoroughly.
    - Note the requirement in Section G on the Government Paperwork Elimination Act to identify Paperwork Reduction Act control numbers from information collections tied to this investment.
- Part III, Cost, Schedule, and Performance Goals. Performance measures are again important to OMB. This section needs to have meaningful performance measures. A subset of the performance measures for each major system will be input to Table 22-1, in the President Budget that is submitted to Congress.

Exhibit 53 includes a new Part 4 on Grants Management. Give special attention to preparing a good estimate of the per cent of expenditures devoted to IT security. Separately provide a breakdown of IT security expenditures for each Exhibit 53 line entry using the attached spreadsheet format.

Commerce currently identifies 19% of its IT expenditures as "major." OMB has asked that we raise that percentage to 50. My office will work with you over the next week to identify investments that should be re-classified from "significant" to "major." OMB has requested that any system that processes grants be categorized a "major," regardless of expenditure level.

By Monday, August 27, please send your revised Exhibit 300s for all "major" systems, Exhibit 300s for all approved FY 2003 budget initiatives with summary sheet as shown in Attachment 1, and your revised Exhibit 53 for FY 2001, 2002, 2003 by e-mail to Hedy Walters at hwalters@doc.gov. If you have questions contact Lisa Westerback at 202-482-0694 or Hedy at 202-482-0593.

Attachment

cc: Barbara Retzlaff, OB
Michael Sade, OAM
Jim Taylor, OFM
Bob Bair, OFM
Budget Officers
Administrative Officers

Attachment 1

Commerce Information Technology Review Board
Summary Sheet

Operating Unit:		
Office:		
Project Name:		
Life Cycle Costs	Total:	Information Technology:
FY 2003 Costs	Total:	Information Technology:
Project Description:		

ALLOCATION OF IT SECURITY COSTS

CATEGORY*	FY2001	FY2002	FY2003	TOTAL
1. Program Planning, Management and Oversight				
A. NOAA personnel ($K)				0
B. Other costs ($K)				0
Subtotal ($K):	0	0	0	0
2. Evaluation and Testing				
A. NOAA personnel ($K)				0
B. Other costs ($K)				0
Subtotal ($K):	0	0	0	0
3. Technical Controls				
A. NOAA personnel ($K)				0
B. Other costs ($K)				0
Subtotal ($K):	0	0	0	0
4. Security Awareness, Training, and Education				
A. NOAA personnel ($K)				0
B. Other costs ($K)				0
Subtotal ($K):	0	0	0	0
5. Incident Response				
A. NOAA personnel ($K)				0
B. Other costs ($K)				0
Subtotal ($K):	0	0	0	0
TOTAL INVESTMENTS ($K):	0	0	0	0

***Category Definitions:**

Program Planning and Management:
- Policy Development
- Security Program Management
- Security Plan Development
- Continuity of Operations Plan Development
- Accreditation Process
- Security Program Compliance Reviews

Evaluation and Testing:
- Risk Assessments
- Vulnerability Assessments
- Penetration Testing
- Continuity of Operations Testing

Technical Controls:
- System-level Technical Controls
- Firewalls
- Intrusion Detection Systems
- Virus Detection Software
- Hardware/Software
- Continuity of Support - backup/alternate/hot sites, off-site storage

Security Awareness, Training, and Education:
- General User Awareness
- Special Security Training and Education (specific system security controls)
- Network/system Administrator Training and Education
- ITSO/ITSSO Training and Education

Incident Response: actions responding to security incidents

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

JUL 27 2001

MEMORANDUM FOR: Secretarial Officers
Heads of Operating Units

FROM: Donald L. Evans

SUBJECT: High Priority to Information Technology (IT) Security

The Department of Commerce has many diverse missions that impact the daily lives of the American people in many ways. Much of our work on behalf of our citizens is reliant, either directly or indirectly, on the quality and integrity of our data and IT systems. In order to assure that our data and IT systems are adequately protected against risks of loss, misuse, or unauthorized access, it is important that we give a high priority to IT security.

I recently approved a new IT management restructuring plan which empowers the Department Chief Information Officer (CIO) to address IT security Commerce wide. It is essential that you work closely with and support your operating unit CIO with respect to IT security. Allocation of sufficient resources at the operating unit level is necessary for the protection of Commerce data and IT systems.

I expect each of you personally to invest as much time as necessary to assure full compliance with my IT security improvement directives.

THE SECRETARY OF COMMERCE
Washington, D.C. 20230

JUN 13 2001

MEMORANDUM FOR Secretarial Officers
Heads of Operating Units

FROM: Donald L. Evans

SUBJECT: Strengthening Commerce Information Technology Management

In order to manage and be accountable for public assets and to ensure that limited public dollars are being spent for the most critical needs, we must strengthen the management of information technology (IT) in the Department. IT is important to the Department's mission, and IT expenditures represent a significant part of the Department's budget. Effective IT capital investment planning is critical.

Therefore, I request that you implement the Department of Commerce IT Restructuring Plan, a copy of which is attached. Department-wide implementation of this plan will be overseen by the Department's Chief Information Officer.

Attachment

DEPARTMENT OF COMMERCE

Information Technology (IT) Restructuring Plan

In order to strengthen the Department's management of IT:

1. Each operating unit (and major NOAA line offices) will establish a Chief Information Officer, who will report to the head of the operating unit (Under Secretary, Assistant Secretary, Director, or Administrator) or principal Deputy, and to the Departmental CIO.

2. Operating unit CIOs will be responsible for advising the operating unit on all aspects of IT and for developing and recommending policies for managing IT within the operating unit, consistent with Departmental policies and guidelines.

3. Operating unit CIOs will have line authority and responsibility for centralized IT functions. At a minimum, those functions that will be centralized under the CIOs will be:

   a. IT for Office Support
   b. Telecommunications Networks
   c. Administrative Data Centers
   d. Website Support
   e. IT for Forms and Records
   f. IT for Administration, including Human Resources, Purchasing, Security and Facilities Management.

4. The performance plan for each operating unit CIO will be established and evaluated by the Head of the Operating Unit (or that person's designee) in consultation with the Department CIO (or, in the case of NOAA line offices, the NOAA CIO as delegated by the Department CIO).

5. The operating unit CIO will establish and evaluate a critical element of the performance plan for the most senior IT manager for those IT personnel who do not report to the CIO. The intent of this element is to ensure that all IT personnel in an operating unit have in their management chain someone who is responsible to the CIO for improvements in IT management.

6. All employees of the Department who perform IT work will have an element in their performance plan that evaluates their improvement in the way their IT work is performed. This element will be established and evaluated by the employee's direct supervisor. The purpose of this element is to require employees who perform IT work as part of their job (including researchers, economists, etc.) to improve how their IT work is done, similar to the way we have used the "diversity" critical element.

7. The operating unit CIO must concur in the budgeting and expenditure of funds for IT by the operating unit. In the event the operating unit CIO does not concur, the Head of the Operating Unit will be the deciding official. The operating unit CIO will provide guidelines to allow small and routine expenditures to be made without further explicit approval.

8. The Department CIO will report to the Secretary. The performance plans for both the CIO and CFO/ASA will include elements ensuring continued strong cooperation between their offices. The CIO's performance plan will be changed to reflect the increased responsibility and authority due to the reorganization.

9. Within sixty (60) days of the approval of this reorganization, the head of each operating unit will submit a plan for the approval of the Assistant Secretary for Administration and the Department Chief Information Officer detailing how these recommendations will be implemented in the operating unit.

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
I. **The Department's IT Security Policy Needs to Be Revised and Expanded**	It has been OMB's practice to issue major updates to policy only at significant intervals, and in between, issue memoranda to update or modify policy, as necessary. While we agree that it is time for Commerce to update its IT security policies, we feel that it is important to note that we have followed the same basic principle as OMB, in that we have issued updates and addressed new issues in the form of memoranda.
We recommend that the CIO revise the outdated program policy and incomplete issue-specific policy for the Department's IT security program as soon as possible. The revised policy should include:	We have recently received the authority to fill the vacancy on the IT Security staff, and the position is open as of this writing. It will, therefore, be feasible to begin updating the policy in the immediate future.
1. Current federal criteria for the format and content of IT security plans, as specified in NIST SP 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.	Our current policy, per the DOC CIO's memorandum to operating unit heads of June 9, 1999, requires that security plans follow NIST SP 800-18. The next revision of the security policy in the IT Management Handbook will incorporate provisions of this memo.
2. A provision for alternatives to formal certifications for lower risk systems, such as risk analyses or audits.	We agree in part. The Department's revised policy will require certification efforts commensurate with the criticality of the system. However, it is imperative to consider interconnections to systems of higher risk, and we plan to require this element in any certification process, even for systems of apparent lesser risk. Given the lack of priority and funding by the Clinton Administration

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
	in the area of critical infrastructure protection, we must disagree with the OIG assertion that using information security assessments scheduled to be performed on the Department's critical infrastructure systems would result in more systems being certified, while realizing significant savings. In the event that the Bush Administration raises the priority of critical infrastructure protection through the application of funding, we will take advantage of assessments gained through this avenue.
3. A provision for self-verification reviews for general support systems with lower risk.	We agree. The Department's revised policy will require verification reviews commensurate with the criticality of the system, with the requirement to consider interconnections to systems of higher risk.
4. A requirement to notify the OIG in the event of IT security incidents involving the Department's systems, networks, or web sites or any other IT security matter that involves the manipulation, destruction, or loss of data or systems, or denial of service including repeated penetration attempts from the same Internet address.	We agree and will take action to ensure that it is carried out. However, there is still a large degree of latitude, which we believe will continue to cause misunderstandings in the future, especially in the area of thresholds for denial of service and repeated attempts. We believe that further discussion is necessary to come to a reasonable understanding. We expect the operating units to have a wide range of opinions as to what that threshold should be and consensus will be a challenge. We would appreciate more specific guidance in this area.
5. A change in risk assessment emphasis from complex, documented assessments that focus on specific risks to general risk assessments. Also, risk assessments should be	We agree in part. The Department's revised policy will require risk assessments commensurate with the criticality of the system. However, we do not understand your distinction between specific

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
linked in policy and practice to vulnerability assessments required under Presidential Decision Directive 63.	risks and general risks, and would appreciate a clarification. Efforts required by PDD-63 are not separate, but rather a prioritization under the overall IT Security Program. The Department's revised policy will reflect that.
6. Guidance to operating units that manual operations are generally not a viable backup option for the Department's systems.	We agree. The Department's revised policy will discourage manual operations, and will specify the conditions of low volume and an assurance that automated operations can be resumed in a relatively short time frame.
7. A requirement that individuals be trained on how to fulfill their security responsibilities before they are permitted access to sensitive systems.	We agree and will update Departmental policy accordingly. The following was proposed, in part, as an element in the CIO performance plans: Require a computer security awareness briefing for new employees before they are allowed access to your IT systems.
8. A change in the Designated Approving Authority for sensitive systems from the CIO to a management official having responsibility for the function supported by the system.	We agree. We propose a change in Departmental policy that would require the certification process to be done in coordination with the operating unit CIO, then have the OU CIO present the risks in an executive-level fashion to the program official, to ensure that they can be understood in a business context, and in a language appropriate to the position and technical understanding of the program official. The program official would then approve the system for processing, or require additional risk mitigation, as appropriate.

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
9. A requirement for operating units to include IT security deficiencies as material weaknesses pursuant to OMB Circular A-123 and FMFIA, and to include in their information resources management plans summaries of agency IT security plans pursuant to the Computer Security Act of 1987. Links should also be added to other federal IT security-related criteria, such as OMB Memorandum 00-07, the Clinger-Cohen Act, *Presidential Decision Directive 63*, the Government Performance and Results Act, the Chief Financial Officer's Act, and the Federal Financial Management Improvement Act.	In principle, we agree with your recommendation to report security deficiencies as material weaknesses when there is no assignment of security responsibility, no security plan, or no accreditation. However, in practice, we would be reporting 91.7 % of the Department's IT systems. We suggest a two-part alternative: 1. That such reporting begin after a reasonable period of notice and time to comply. We propose one year, and 2. The use of a senior management council as a forum for assessing and monitoring deficiencies in management controls. This is suggested in OMB Circular A-123, and would provide Commerce with a means of determining the risk within each instance of deficiency, and with the means to declare a lesser deficiency that could be handled within the Department. This council could recommend to the Secretary which deficiencies are deemed to be material to Commerce as a whole, and should therefore be included in the annual Integrity Act report to the President and the Congress. This council could also be used to determine when sufficient action has been taken to declare that a deficiency has been corrected. We would invite the

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
	OIG to attend and give counsel at these discussions. In regard to your recommendation that operating units include in their information resources management plans summaries of agency IT security plans: We currently require that operating units identify strategies to address IT Security in their annual IT Strategic Plan, and an update of their compliance with the Department IT Security Program requirements in their annual Operational IT Plan. We are not clear how we fail to meet this requirement. Also, if more detail is required, we are uncertain how this can be accomplished without revealing security weaknesses in a public document. We would appreciate further guidance concerning the approach and level of detail expected in such a reporting.
10. Issue-specific IT security policy on Internet usage, e-mail, web security, and communications.	We agree and will ensure that these issues are included in the self assessment. See II.1 below.
II CIO Has Taken Steps to Improve IT Security, But Additional Efforts Are Needed	
In addition to the oversight of operating unit self-assessments using the CIO Council Framework, we recommend that the CIO commit to an operating unit compliance review program that extends beyond the FY 2001 and 2002 requirement of the recent Government Information Security Reform Act. Reviews should begin as soon as possible and should ensure that operating units:	We agree that the requirements of the Government Information Security Reform Act need to be continued into future years. We agree that better compliance review is necessary. Unfortunately, even with the addition of one IT Security staff member, hands-on compliance review of operating unit systems by the OCIO in FY

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
	2001 will not be possible in time to fulfill the OMB requirements of this Fall. Therefore, for this year, we plan to use the Federal CIO Council's Security Assessment Framework in a self-assessment model. We will then measure the success of this approach and plan for future years accordingly. It is our goal, in future years, to add hands-on compliance reviews as resources permit.
1. Have program-level, issue-specific, and system-level policy in place that complies with federal IT security policy and the Department's revised program-level policy.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
2. Implement formal IT security awareness and training programs.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
3. Develop incident response capabilities.	We agree. The draft questionnaire prepared by NIST in support of the Framework addresses this issue.
4. Report deficiencies in IT security as material weaknesses pursuant to OMB Circular A-123 and FMFIA.	See I.9 above.
5. Include IT-related procurement specifications for hardware, software or services, to ensure that they include adequate security requirements and/or specifications that are commensurate with the sensitivity of the system, and that security requirements are included in operating unit budgets. The CIO should work with the Department's Office of Acquisition Management and the Office of Budget to ensure	We agree and will ensure that these issues are included in the self assessment. We agree. This is already being done for major systems that require an Exhibit 300B submission to OMB. We will begin liaison with the Office of Acquisition Management and the Office of Budget to ensure implementation for other systems.

Additional Focus Needed on Information Technology Security Policy and Oversight
Draft Inspection Report No. OSE-13573/February 2001

Draft Comments on Recommendations

March 29, 2001

OIG Recommendation	OCIO Comment
implementation.	
6. We also recommend that the review program include procedures to review on a sample basis operating unit IT security documents to determine that:	We agree that quality of assessments and plans should be emphasized in addition to quantity.
a. IT security plans are prepared for all sensitive systems and that they comply with NIST SP 800-18.	We agree and will begin a program to review IT Security plans on a sample basis as resources permit.
b. Systems are accredited and that a management official was involved in the accreditation process.	We agree. We have recognized through your review, and that of the GAO, that our accreditation process needs improvement. We plan to require that the CIO be the liaison between the certification and accreditation processes in order to introduce a technical to business translator.
c. Verification reviews of individual systems are conducted at least every three years or when significant modifications are made to systems and that the scope of the reviews is appropriate based on system risk.	We agree and will ensure that these issues are included in the self assessment.
d. Systems are audited periodically for illegal software or that some other mechanism exists for ensuring that only legal copies of software are being used.	We agree and will ensure that these issues are included in the self assessment.

List of Department of Commerce systems included in GAO review*

*data as of March 30, 2001

	Bureau	System name	Security Plan	Documented Risk Assessment
1	BXA	NEC Technical Information Center Training LAN	(draft 6/30/99)	
2	BXA	Chemical Weapons Convention (CWC) Information Management System	(draft 3/2000)	
3	BXA	Export Control Automated Support System (ECASS)	(draft 3/2000)	
4	BXA	BXA Communications Infrastructure (BCI) Network	6/1999	
5	BXA	Defense Priorities Allocation System		
6	BXA	Export License Application and Information Network		
7	BXA	Amanda Phone System		
8	BXA	Secure Automated Screening System		
9	BXA	Boycott Reporting System		
10	BXA	Systems for Tracking Export License Applications		
11	BXA	Multipurpose Archival Records Retrieval System (MARRS)		
12	BXA	Net Facts		
13	BXA	Correspondence Tracking System		
14	BXA	EA Personnel System		
15	BXA	Export License Voice Information System (ELVIS)		
16	BXA	Fast Fax		
17	BXA	Open source Data Base Screening		
18	BXA	Security Database		
19	BXA	Shippers Export Declaration System		
20	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		

List of Department of Commerce systems included in GAO review*

*data as of March 30, 2001

21	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
22	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
23	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
24	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
25	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
26	BXA	Name unknown - BXA officials stated they had 26 total sensitive systems, but did not provide a complete listing		
27	EDA	Operational Planning and Control System (OPCS)		
28	EDA	Commerce Administrative Management System (CAMS)/Core Financial System (CFS) Grant Accounting System		
29	EDA	General EDA-wide General Support Systems		
30	EDA	Loan Billing and Management System		
31	EDA	EDA LAN/WAN		
32	EDA	EDA Virtual Private Network		
33	ESA	STAT-USA, 3 modules • STAT-USA Internet • STAT-USA Account Manager (SAM) • USA Trade Online	7/2000	
34	ITA	Client Management System (CMS)	12/1999	
35	ITA	Trade Policy Information System (TPIS)	6/2000	

List of Department of Commerce systems included in GAO review*

*data as of March 30, 2001

36	ITA	ITA Headquarters LAN	(draft 12/13/99)	(7/2000)
37	ITA	US&FCS Network		(4/2000)
38	ITA	Message Processing System (MPS)		
39	ITA	Central Records Information Management System		
40	ITA	Federal Financial System		
41	ITA	Textiles Information Management System		
42	MBDA	Opportunity System		
43	MBDA	Phoenix System		
44	MBDA	Performance System		
45	MBDA	Internet Service Cluster		
46	MBDA	MBDA's LAN/WAN		
47	NTIA	NTIA LAN	3/26/01	
48	NTIA	Frequency Records & Management System		
49	NTIA	Grant Monitoring System		
50	NTIA	NTIA Time Keeping Systems		
51	OS	OS LAN	(draft 9/2000)	
52	OS	CAMS Support Center (CSC): CAMS IT Security Plan 3 modules • CFS • Commerce Purchase Card System (CPCS) • CSC LAN	11/1999	(9/1999)
53	OS	Office of Computer Services (OCS): System Security Plan for OCS LAN	2/2000	
54	OS	Office of Security: Security Information Management System		(draft 7/1999)
55	OS	Office of Acquisition Management (OAM): Small Purchases System		
56	OS	OAM: Commerce Procurement Data System (CPDS)		

List of Department of Commerce systems included in GAO review*

*data as of March 30, 2001

57	OS	Real Estate and Space Management Information System (RSMIS)		
58	OS	Budget and Performance Reporting System		
59	OS	Office of Budget (OB): Time and Attendance (T&A) System		
60	OS	T&A System - PPE		
61	OS	Office of Management & Organization (OMO): T&A System		
62	OS	Commerce Opportunities On-Line		
63	OS	General Workforce End-of-Year Rating Cycle		
64	OS	Office of Human Resource Management (OHRM): Executive Resource Data System		
65	OS	Human Resources Data System		
66	OS	Performance Appraisal Software System		
67	OS	Senior Executive Service End-of-Year Rating Cycle		
68	OS	Worker's Compensation System		
69	OS	Electronic Official Personnel Folder		
70	OS	Automated Classification System		
71	OS	Performance Payout and Annual Comparability Increase System		
72	OS	Personal Property System		
73	OS	Electronic System for Personnel		
74	OS	Executive Resources Information Tracking System		
75	OS	Honor Awards Documentation and Selection		
76	OS	Incident Response Information Management System		
77	OS	EEO Tracking System		
78	OS	Personnel Security Database		
79	OS	Reemployment Priority List & Priority Placement System		

List of Department of Commerce systems included in GAO review*

*data as of March 30, 2001

80	OS	Telecommunications Management Information System (TMIS)		
81	OS	TRAQ Personal Property Management System		
82	OS	Web Page		
83	OS	WinCITS		
84	OS	Remote Entry T&A System		
85	OS	SES Bonus Pool System		
86	OS	T&A Data Transmission		
87	OS	Budget Status Report		
88	OS	CD-435 System		
89	OS	Checkbook		
90	OS	HORIZON		
91	OS	OCLC		
92	OS	Mail Management System		
93	OS	COGNOS NFC Data Reporting System		
94	OS	FARS		

Summary:

Total systems **94**

Systems with finalized Security Plans:	7
Systems with draft Security Plans:	5
Systems with no (finalized) Security Plan:	87
Systems with finalized risk assessments:	3
Systems with draft risk assessments:	1
Systems with no (documented) risk assessment:	90

Department of Commerce IT Security Task Force

Goal:	To strengthen IT Security management in the Department of Commerce, by developing a comprehensive IT Security Program for the Department of Commerce and its Operating Units To develop recommendations for action by the Commerce CIO and Operating Unit CIOs
Principal Tasks:	Develop a comprehensive IT Security program plan, including recommendations on functions to be carried out at the Department level and by the Operating Units Identify the highest priority IT security tasks not currently being done, and recommend that Commerce CIO begin implementing them immediately in parallel with the continued Task Force review
Time frame:	July 23, 2001 - September 30, 2001

Commerce IT Security Task Force
Kickoff Meeting

Monday, July 23, 3:00-5:00 p.m.
Room 6057, HCHB

Membership

Tom Pyke, Acting Commerce CIO
Mike Lombard, Commerce OCIO
Paulette Dawson, Commerce OCIO

Gordon Fields, Commerce, OGC
Wil Acevedo, Commerce, OSY

Rick Swartz, Census CIO
Pat Heinig, BXA CIO
Renee Macklin, ITA CIO
Sarah Maloney, NTIA CIO

Tim Ruland, Census ITSO
Becky Vasvary, NOAA ITSO
Colin Brown, BEA ITSO

Fran Nielsen, NIST
Conrad Lovely, NOAA
Linda Laboski, NOAA

JoAnn Craycraft, NSA
Bill Johnston, NSA

Meeting Notes

Tom Pyke opened the meeting and thanked all for attending and agreeing to participate on the task force. He discussed the charter and said that basically the group needs to develop the structure of a comprehensive IT security program for the Department. He passed out a point paper on the GAO report and addressed the issues raised.

Next Mike Lombard presented the baseline Commerce IT security program. Followed by Becky Vasvary who presented the NOAA baseline IT security program.

Tom passed out a paper for discussion entitled: "Elements of a Balanced IT Security Program. Many said it was a good starting point and a discussion of the elements ensued.

Basically, the group agreed to form two working groups to concentrate on two areas: (1) IT Security Program Structure and (2) Priority Actions.

(1) The IT Security Program Structure Working Group would use the elements identified in the paper mentioned above and whatever other sources they deemed appropriate to come up with a proposed program structure. Members of this group:

- Fran Nielsen, NIST, Chair
- Sarah Maloney, CIO - NIIA
- Renee Macklin, CIO - ITA
- Becky Vasvary, NOAA
- Bill Johston, NSA
- JoAnn Craycraft, NSA
- Mike Lombard, Commerce OCIO
- Paulette Dawson, Commerce OCIO

(2) The Priority Action Working Group would identify what we can do now to improve our IT security posture. Members of this group:

- Pat Heinig, CIO, BXA, Chair
- Sarah Maloney, CIO, NTIA
- Tim Ruland, Census
- Mike Lombard, Commerce OCIO
- Paulette Dawson, Commerce OCIO

Action items:

- Mike Lombard will follow up with Treasury, IRS & DISA for possible presentations to the task force.

- The working groups will come back to the next meeting with a "report."

Next Meeting: Thursday, August 9, 10 a.m., Room 6057