

ENHANCING COMPUTER SECURITY: WHAT TOOLS WORK BEST

HEARING

BEFORE THE
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY
OF THE
COMMITTEE ON
GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

MARCH 29, 2000

Serial No. 106-181

Printed for the use of the Committee on Government Reform



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

U.S. GOVERNMENT PRINTING OFFICE

69-819 DTP

WASHINGTON : 2001

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: (202) 512-1800 Fax: (202) 512-2250
Mail: Stop SSOP, Washington, DC 20402-0001

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York	HENRY A. WAXMAN, California
CONSTANCE A. MORELLA, Maryland	TOM LANTOS, California
CHRISTOPHER SHAYS, Connecticut	ROBERT E. WISE, JR., West Virginia
ILEANA ROS-LEHTINEN, Florida	MAJOR R. OWENS, New York
JOHN M. McHUGH, New York	EDOLPHUS TOWNS, New York
STEPHEN HORN, California	PAUL E. KANJORSKI, Pennsylvania
JOHN L. MICA, Florida	PATSY T. MINK, Hawaii
THOMAS M. DAVIS, Virginia	CAROLYN B. MALONEY, New York
DAVID M. McINTOSH, Indiana	ELEANOR HOLMES NORTON, Washington, DC
MARK E. SOUDER, Indiana	CHAKA FATTAH, Pennsylvania
JOE SCARBOROUGH, Florida	ELIJAH E. CUMMINGS, Maryland
STEVEN C. LATOURETTE, Ohio	DENNIS J. KUCINICH, Ohio
MARSHALL "MARK" SANFORD, South Carolina	ROD R. BLAGOJEVICH, Illinois
BOB BARR, Georgia	DANNY K. DAVIS, Illinois
DAN MILLER, Florida	JOHN F. TIERNEY, Massachusetts
ASA HUTCHINSON, Arkansas	JIM TURNER, Texas
LEE TERRY, Nebraska	THOMAS H. ALLEN, Maine
JUDY BIGGERT, Illinois	HAROLD E. FORD, JR., Tennessee
GREG WALDEN, Oregon	JANICE D. SCHAKOWSKY, Illinois
DOUG OSE, California	
PAUL RYAN, Wisconsin	BERNARD SANDERS, Vermont (Independent)
HELEN CHENOWETH-HAGE, Idaho	
DAVID VITTER, Louisiana	

KEVIN BINGER, *Staff Director*

DANIEL R. MOLL, *Deputy Staff Director*

DAVID A. KASS, *Deputy Counsel and Parliamentarian*

LISA SMITH ARAFUNE, *Chief Clerk*

PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON GOVERNMENT MANAGEMENT, INFORMATION, AND TECHNOLOGY

STEPHEN HORN, California, *Chairman*

JUDY BIGGERT, Illinois	JIM TURNER, Texas
THOMAS M. DAVIS, Virginia	PAUL E. KANJORSKI, Pennsylvania
GREG WALDEN, Oregon	MAJOR R. OWENS, New York
DOUG OSE, California	PATSY T. MINK, Hawaii
PAUL RYAN, Wisconsin	CAROLYN B. MALONEY, New York

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

J. RUSSELL GEORGE, *Staff Director and Chief Counsel*

MATT RYAN, *Senior Policy Director*

BRYAN SISK, *Clerk*

TREY HENDERSON, *Minority Counsel*

CONTENTS

	Page
Hearing held on March 29, 2000	1
Statement of:	
Brock, Jack L., Jr., Director, Governmentwide and Defense Information Systems, U.S. General Accounting Office, accompanied by Jean Boltz, U.S. General Accounting Office	7
Collier, Paul, division general manager, Identix, Inc	39
Nelson, Dave, Deputy Chief Information Officer, National Aeronautics and Space Administration	27
Letters, statements, et cetera, submitted for the record by:	
Brock, Jack L., Jr., Director, Governmentwide and Defense Information Systems, U.S. General Accounting Office, prepared statement of	13
Collier, Paul, division general manager, Identix, Inc, prepared statement of	42
Horn, Hon. Stephen, a Representative in Congress from the State of California, prepared statement of	3
Nelson, Dave, Deputy Chief Information Officer, National Aeronautics and Space Administration, prepared statement of	30
Turner, Hon. Jim, a Representative in Congress from the State of Texas, prepared statement of	5

ENHANCING COMPUTER SECURITY: WHAT TOOLS WORK BEST

WEDNESDAY, MARCH 29, 2000

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON GOVERNMENT MANAGEMENT,
INFORMATION, AND TECHNOLOGY,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

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

Present: Representatives Horn and Turner.

Staff present: J. Russell George, staff director and chief counsel; Matt Ryan, senior policy director; Bonnie Heald, director of communications; Bryan Sisk, clerk; Ryan McKee, staff assistant; Trey Henderson, minority counsel; and Jean Gosa, minority assistant clerk.

Mr. HORN. A quorum being present, the Subcommittee on Government Management, Information, and Technology will come to order.

This is the second in a series of hearings to examine computer security concerns in the Federal Government. The subcommittee's first hearing 3 weeks ago shed light on two important topics, awareness of the increasing number of computer threats against Federal and private computer systems, and the need for a coordinated Federal effort to meet this challenge.

History is full of claims of developing the ultimate weapon, whether it was a battleship, a supersonic fighter jet, or a weapon capable of massive destruction. Today's computer systems and networks provide the newest frontier, the weaponry of knowledge. With only a few keystrokes, computers provide massive amounts of information, information that only a decade ago would have taken months or years to compile. It is, of course, imperative that these computers and the wealth of information they contain be protected.

Nearly all computer networks are vulnerable to attack at some level, but steps can be taken to prevent or reduce those intrusions. Organizations must focus on two areas, physical security and information security. No one would buy an expensive house, furnish it, then walk away leaving the doors wide open. Physical assets must be protected. Yet many organizations fail to take basic precautions to protect either their facilities or their computer systems.

Electronic government and electronic commerce trends should continue to dictate the way important data are exchanged. From tax refunds and health records to credit card purchases and Social

Security numbers, organizations must demonstrate that the information flowing into their computers is secure. Tools are available to help organizations and citizens protect their computers against unwanted and unruly intruders. However, they must be carefully used to ensure that they lead to meaningful improvement. Today our witnesses will talk about some of these tools that can enhance computer security at little or no cost. We welcome our panel of witnesses. We look forward to their testimony.

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

DAN BURTON, INDIANA
CHAIRMAN
BENJAMIN A. GILMAN, NEW YORK
CONSTANCE A. HOBELLA, MARYLAND
CHRISTOPHER SHAYS, CONNECTICUT
E. J. SCHLEHTMANN, FLORIDA
JACOB K. SISK, NEW YORK
STEVEN HORN, CALIFORNIA
JON H. ROSEN, FLORIDA
THOMAS M. DAVIS II, VIRGINIA
DAVID L. BONIOR, INDIANA
MARK E. SOUDER, INDIANA
JOE SCARBOROUGH, FLORIDA
STEVEN C. LATOURETTE, OHIO
MARTIN "MARK" SANFORD, SOUTH CAROLINA
BOB BARR, GEORGIA
DAN MILLER, FLORIDA
ASB MITCHELL, ARIZONA
LEE TERRY, NEBRASKA
JERRY BOGGS, ILLINOIS
ORREG WALDEN, OREGON
EDOUARD CALIFORNIA
PAUL RYAN, WISCONSIN
JOHN T. DODDLE, CALIFORNIA
HELEN CHENOWETH, IDAHO

ONE HUNDRED SIXTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

Majority (202) 225-5074
Minority (202) 225-5031
TY (202) 225-4952

HENRY A. WAXMAN, CALIFORNIA
RANKED-MINORITY MEMBER
TOM LANTOS, CALIFORNIA
ROBERT E. WISSE, JR., WEST VIRGINIA
MAJOR R. OWENS, NEW YORK
EDOUARD FORTNE, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
PATSY T. MINK, HAWAII
CAROLYN B. MALONEY, NEW YORK
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
CHARA FATTAH, PENNSYLVANIA
ELIJAH E. DIMMICK, MARYLAND
DENNIS J. BOGGS, OHIO
ROD R. BLAGOVICH, ILLINOIS
DANNY K. DAVIS, ILLINOIS
JOHN F. TETNEY, MASSACHUSETTS
JIM TURNER, TEXAS
THOMAS H. ALLEN, MAINE
HAROLD E. FORD, JR., TENNESSEE

BERNARD SANDERS, VERMONT,
RANKED-MEMBER

OPENING STATEMENT

Chairman Stephen Horn,
Subcommittee on Government Management, Information and Technology
"Enhancing Computer Security: What Tools Work Best?"
10 a.m., March 29, 2000

A quorum being present, the Subcommittee on Government Management, Information, and Technology will come to order.

This is the second in a series of hearings to examine computer security concerns in the Federal Government. The subcommittee's first hearing, three weeks ago, shed light on two important topics: awareness of the increasing number of computer threats against Federal and private computer systems, and the need for a coordinated Federal effort to meet this challenge.

History is full of claims of developing the "ultimate weapon," whether it was a battleship, a supersonic fighter jet or a weapon capable of massive destruction. Today's computer systems and networks provide the newest frontier -- the weaponry of knowledge. With only a few keystrokes, computers provide massive amounts of information -- information that, only a decade ago, would have taken months or years to compile. It is, of course, imperative that these computers, and the wealth of information they contain, be protected.

Nearly all computer networks are vulnerable to attack at some level, but steps can be taken to prevent or reduce those intrusions. Organizations must focus on two areas: physical security and information security. No one would buy an expensive house, furnish it, and then walk away, leaving the doors wide open. Physical assets must be protected. Yet many organizations fail to take basic precautions to protect either their facilities or their computer systems.

Electronic government and electronic commerce trends should continue to dictate the way important data is exchanged. From tax refunds and health records to credit card purchases and social security numbers, organizations must demonstrate that the information flowing into their computers is secure. Tools are available to help organizations and citizens protect their computers against unwanted and unruly intruders. However, they must be carefully used to ensure that they lead to meaningful improvement. Today, our witnesses will talk about some of these tools that can enhance computer security at little or no cost.

We welcome our witnesses and look forward to their testimony.

Mr. HORN. It is now my pleasure to call on the ranking member of the subcommittee, Mr. Turner of Texas, for an opening statement.

Mr. TURNER. Thank you, Mr. Chairman. This is the second in a series of hearings that the chairman has designated to discuss the issue of computer security in the Federal Government, and it is apparent to all of us that we have become increasingly dependent upon computer systems and the Internet. It represents one of our greatest strengths, but perhaps also one of our greatest weaknesses and vulnerabilities.

While we rely extensively on electronic data, we have become increasingly vulnerable. The General Accounting Office has stated that our computer security system is not where it needs to be to protect ourselves from cyberinvaders. We lack an overall comprehensive program in the Federal Government to protect our computer system, and billions of dollars in Federal assets and large amounts of sensitive data are at risk to the threat of hackers, both foreign and domestic.

I am pleased that the chairman has chosen to focus upon this issue of computer security, and I look forward to hearing from each of our witnesses today.

Mr. HORN. I thank the gentleman.

[The prepared statement of Hon. Jim Turner follows:]

Statement of the Honorable Jim Turner
GMIT Hearing: "Enhancing Computer Security: What
Tools Work Best"
03/29/00

Thank you, Mr. Chairman. This is the second in a series of hearings this subcommittee is conducting on computer security. As I mentioned in our last hearing on this issue, computer security is broader and potentially poses a greater threat to our country than the Y2K challenge. More than any other nation, the United States depends on interconnected computer systems - including the Internet -- to support critical operations and services both in the public and private sectors. Computers perform functions that are essential to the national welfare and directly affect the lives of millions of individuals.

While beneficial and efficient, this reliance on electronic data has left us highly vulnerable. The GAO has stated that our computer security system is not where it needs to be to protect ourselves from cyber-invaders. Our nation lacks an overall comprehensive computer security management program. Therefore, billions of dollars of federal assets and large amounts

of sensitive data are at risk to the threat of hackers -- both foreign and domestic.

The purpose of this hearing is to focus on the precautionary measures that agencies' can take to shield intruders from their networks. These safeguards include having network administrators employ more rigorous "password" techniques, the prohibition of mass email distributions, and the use of encryption and biometrics. These measures represent our first line of defense against attackers.

I am pleased that the Congress has made this issue computer security a priority. I thank the chairman for his focus on this matter and welcome the witnesses that have come here today for their time and expertise.

Mr. HORN. Let me tell you the procedure here. Some of you have testified here before, but when we introduce you, and we will go in the order it is on the agenda, your statement, as written, is fully in the record. What we would like you to do is spend 5 minutes and at the most 8 or 10 to summarize your statement, not read it to us. We can read. Then we have more time for dialog between the three of you and dialog with the Members here today.

So we, as you know, swear in all witnesses before these subcommittees of government reform, and if you will stand, raise your right hand, we will swear you in.

Anybody that is going to give you advice, swear them in, too.

[Witnesses sworn.]

Mr. HORN. The record will note that three witnesses and one helper affirmed the oath.

So we will now start with Mr. Brock of the U.S. General Accounting Office, part of the legislative branch of Congress, who does a wonderful job on both programmatic and fiscal matters.

Mr. Jack Brock is no stranger to this subcommittee. He is Director of Governmentwide and Defense Information Systems for the U.S. General Accounting Office, otherwise known as GAO.

Mr. Brock.

STATEMENT OF JACK L. BROCK, JR., DIRECTOR, GOVERNMENTWIDE AND DEFENSE INFORMATION SYSTEMS, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY JEAN BOLTZ, U.S. GENERAL ACCOUNTING OFFICE

Mr. BROCK. Thank you very much, Mr. Chairman. Good morning to you. Good morning, Mr. Turner.

I would like to note that my license plates say Native Texan.

I would also like to introduce Ms. Jean Boltz. Ms. Boltz is a senior manager in my group and actually directs a great deal of our computer security work.

Mr. HORN. That's B-O-W-L-T-Z.

Mr. BROCK. B-O-L-T-Z.

Mr. HORN. I am glad I asked.

Mr. BROCK. I know you have had a prior hearing on computer security, and in that hearing you discussed the importance of good security, but good computer security is important to every facet of government operations. It assures the integrity and the confidentiality of information and key processes. It is important to national security. It is important to other critical operations. It is important in assuring the integrity of transactions between the government and its citizens; and as e-commerce and e-government become more prevalent, it is the cornerstone of making sure that those services actually achieve the objectives of better government, more efficient government, more productive government.

What we found, though, in our work, as you have noted, is that at virtually every major agency that we go to computer security, the computer security practices within those agencies doesn't match the importance of the topic. We or other independent auditors whose work we reviewed have found serious computer security weaknesses in virtually every major Federal agency, and these weaknesses threaten or potentially threaten the ability of these agencies to protect the confidentiality of key data, to perform criti-

cal operations, and assure the integrity of important financial and data transactions. I have identified several examples in my testimony, but I would just like to quote here what we found at EPA, which is our most recent report.

We found serious and pervasive problems that essentially render EPA's agencywide information security program ineffective. We found that the current security program planning and management is largely a paper exercise that has done little to substantially identify, evaluate, and mitigate risk to the agency's data and systems.

What we found essentially, Mr. Chairman, that EPA has a central network, and most of EPA's business functions operate off that network. We were able to penetrate the firewall, which was largely ineffective, penetrate limited access controls, and essentially could have had access to most of the information and processes that ran throughout the entire agency. So the entire agency in this case was vulnerable.

EPA is not alone. Recent reports at DOD, at NASA—Mr. Nelson will be talking about that in a moment—the State Department, the National Finance Center, the Veterans Administration all had serious weaknesses. I would, at the risk of preempting Mr. Nelson, say that they have made substantial strides in improving their program, and our limited followup work has substantiated those improvements.

I would like to spend just a moment, if I could, going over the common problems that we find at agencies, and we have a chart that I would refer you to. Mr. Mike Gilmore is up there handling the charts.

First of all, computer security programs have to support the organizational mission and goals of the agency. They can't be divorced from what the agency does, or they are not relevant.

Running across the agency is an entitywide security program planning and management. This is what assures the relevancy of your computer security program to what you are trying to achieve at the agency. And then under that we have found a series of problems that are present in most of our reviews. First of all, many agencies do not have relevant security program planning and management, and we are going to talk about that in a little bit, but that's the root of the problem. When you look at access controls—access controls, you were talking about a house, access controls represent the fence around the house. They represent the lock on the door. They are not in place.

Here we are talking mainly about processes that provide authentication that you are who you say you are and, second, that limit your rights to material that's relevant to you.

Software development and change controls. We are actually doing an assignment for you right now and we are meeting with your staff next week to go over the results of that. That means that when you change software, when you make changes in code, or when new software is introduced, that is tested to make sure that you are not maliciously—you are inadvertently introducing new weaknesses into your application, we find that to be a common problem in many agencies, where that testing is not done, and weaknesses are then inserted into an application that was previously strong.

The next one is on service continuity controls, there you want to maintain the ability to recover from disaster, or if the worst happens, that you are able to take strides to recover your operations and to move forward. Many agencies that we have gone to do not have good service continuity controls, would not be able to reconstruct their principal systems, and would have difficulty bringing—coming back up to speed in an acceptable amount of time.

System software controls, these are really sort of the heart and brains of many systems. These are the basic operating systems, the utilities, that if you don't have good controls over these, a hacker or an intruder can go in and assume control over the entire network by becoming a systems administrator and assuming higher powers than he or she should.

And then finally segregation of duties, if you don't separate the duties from the person who writes the code, the person who inserts the code, the person who tests, the various people who have some element of authorities over the computer security, then you run the risk of empowering one person or a small number of people with too much authorities. It is much like someone who might have authorities over receiving funds, recording those funds, disbursing those funds, and then doing the final accounting. The more you place those duties in the hands of one or a very small number of people, you run the risk of malfeasance.

These are the problems, and you requested that we prepare for you a listing of things that you could do to fix the problems. This really falls into two categories: Is what can you do right now, and what do you need to do on a long-term to have more permanency? Again, I am going to go back to your house example.

Ideally, in a house you have some sort of an alarm system, a fire suppressant system, or whatever. In this case, the house is on fire. Building a fire suppressant system isn't going to do you much good. You have to throw a pail of water on it right now. So we have identified a number of actions that an agency can do now.

Any agency could start on this this afternoon and work on it. So, again, I would refer you to the next table up there, and we have identified a number of things in our work that can be done. The diagram there is designed so that if you take these actions, you will, in fact, be compressing risk and minimizing risk. The first thing you need to do is to increase awareness at all levels, and at the management levels managers need to be aware that this is their information, these are their programs, that poor computer security endangers their activities that they have accountability and responsibility for.

At the user level, you need to make users aware that actions they take in terms of poor password control, sharing passwords, not following agency procedures and processes may, in fact, endanger the system, and at the technical level system administrators need to be aware that if they don't take their actions seriously, if they don't have the right kind of training, if they don't institute software patches or whatever, they are also endangering the system. So there needs to be a much higher level of awareness in most agencies.

Second, you have to make sure that the controls you have work. I know there are going to be tools demonstrated here today. Every

agency has tools, and when we go into agencies, we frequently find that those tools aren't working. They are not turned on. They are not monitored. So agencies are spending money for tools, but they are not using the tools. It is very similar to the set of tools I have in my garage that my father gave me when I moved here from Texas 27 years ago. He said, you will need these tools, and I am sure I do need the tools, but they are still in the tool box.

The same thing with many agencies. Tools are present, but they are not turned on, they are not monitored. You are really not sure that they are working or not.

Third, is implementing software patches. The Carnegie Mellon CERT-CC has said in most of the intrusions they get, most of the incidents that are reported to that organization exploit known vulnerabilities, and for most known vulnerabilities there are existing patches that could be implemented. Many agencies are aware of the patches. They don't follow the advisories that are coming up from the vendors, they don't follow the advisories that are coming out from the CERT, or they don't follow the advisories that come out of their own agencies. By not patching software with known holes, they are leaving in place known vulnerabilities that offer a hacker or an intruder an opportunity to enter into their system.

Next, is to identify and propagate pockets of excellence. Almost every agency we go to, regardless of their overall program and whether it is good or bad, have individual centers or individual programs that work really well. Unfortunately, they are working in concert with other programs that don't work so well, and so sometimes the good effect there is mitigated. But if agencies would identify those pockets of excellence, use those as best practices within the agency, where the agency culture to some degree has already accepted these practices, propagate those across the agency, there would be opportunities for immediate improvements.

Finally, to focus on the most common vulnerabilities first, when we go into agencies, we find throughout the agency that there are a few set of problems that come up time and time again, and surprisingly enough, when we go from one system administrator to the other, they are frequently not aware of the problems that their compatriot down the hall is facing. These need to be shared within the agency. Those need to be addressed first.

Further, we are finding that many of these common problems also exist across agencies, and, again, there is very little sharing of that information across the agency.

If we could turn to the next chart, please.

And these are things agencies can do now. However, computer security is very dynamic. The technology is changing in a hurry. The tools are changing. The techniques that intruders might be using are changing. So the program really has to have a sense of structure in order to make sure that the computer security program is dynamic and, in fact, changes as the threat and risk changes.

About 2 years ago we did a study of leading organizations that had good computer security, and we found a common set of practices in these agencies that we believe are appropriate for Federal agencies to use. In fact, the Federal CIO Council endorsed these

practices, and several agencies have included them within their own policy and structure.

The S. 1993, the computer security bill introduced by Senators Thompson and Lieberman earlier this year, also incorporates these practices, they start off with a central focal point for computer security. Regardless of whether the agency is decentralized or centralized, the central focal point—there was always a central focal point. I think this is true at NASA, where NASA is highly decentralized, and yet Mr. Nelson is the central focal point for security.

The real cornerstone of that, though, is that agencies need to assess the risk and determine needs. Without risk assessment, you can't move to that next box and have effective controls and policies. Your controls and policies need to be built on your risk assessment. They need to be appropriate for the risks that you are facing and, from that, promote awareness. Again, you can increase awareness at all levels on a general level, but at some point the awareness needs to be focused on your exact controls that you are using, how to use them, and on the risks that you are facing so that people throughout the organization can take appropriate action; and then, finally, monitor, and evaluate.

There are two parts to that. First, managers need to do their own self-evaluation so that they can continually assess where the agency is; and second, there needs to be an independent evaluation, something that we might do or the NASA IG might do that would allow both the agency and the oversight agencies or committees such as yourself to take a look at what is going on within the agency. We feel that if this framework was adopted, truly adopted, by agencies, it would go a long ways toward correcting the common problems that we see.

By establishing a framework, we think that an agency can fulfill several key tasks: One, that agency actions are appropriately controlled and coordinated; that the testing tools are appropriately selected and tested; that personnel involved in using the tools are trained; that good practices and lessons learned are shared on an agencywide basis; that controls are systematically tested to ensure that they are effective; and that appropriate risk management decisions are made regarding the best way to address and identify problems.

I would just like to highlight that a little bit. If you do not assess the risk, the controls that you have implemented may or may not be appropriate. You may well be spending too much money. You may not be spending enough money. But almost certainly you will have the wrong kind of control in place, and you really won't address your company's problems.

In conclusion, we also believe, Mr. Chairman, there needs to be some reconsideration of the current legislative framework. The Computer Security Act and A-130, which provides the regulations for the Computer Security Act, really is a system-based piece of legislation. It is based on making every system good and that the accumulation of those good systems will, in fact, represent a good agency program. I don't think that works. It hasn't worked. Legislation needs to be considered that would, in fact, provide a management framework and a management perspective.

Also CSA has two categories of information. It is classified or nonclassified, sensitive or nonsensitive. Actually, information is graduated. Some systems are at a very low level of risk. Some are at a high level of risk, and policies need to be implemented that really reflect that gradation. It doesn't recognize the need for an independent audit, and second—or third, it doesn't recognize the need for more prescriptive guidance that would give agencies more of a framework.

Finally, there is no call for central leadership, somebody that can stir the pot, somebody that can make sure that things are being done, someone that can provide leadership across the government.

That completes the summary of my statement, Mr. Chairman.

Mr. HORN. Thank you very much, Mr. Brock. That's a most helpful summary.

[The prepared statement of Mr. Brock follows:]

United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Government Management,
Information and Technology, Committee on Government
Reform, House of Representatives

For Release on Delivery
Expected at
10 a.m.
Wednesday,
March 29, 2000

FEDERAL INFORMATION SECURITY

Actions Needed to Address Widespread Weaknesses

Statement of Jack L. Brock, Jr.
Director, Governmentwide and Defense Information
Systems
Accounting and Information Management Division



Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss federal information security. Our recent audit findings in this area present a disturbing picture of the state of computer security practices at individual agencies. Our work—and the work of other audit entities—has demonstrated that many agencies' critical operations and processes are at serious risk of disruption because of weak security practices. We have designated computer security as a high-risk area, and the President's plan for protecting critical infrastructure¹ reinforces this designation.

At your request, I will discuss actions agencies can take immediately to strengthen their security programs as well as other actions required to make more fundamental and long-term improvements. Additionally, I will discuss governmentwide actions needed to support and encourage agency progress and congressional oversight of this progress.

**Serious and
Widespread
Weaknesses Place
Critical and Sensitive
Operations and Assets
at Risk**

Computers and electronic data are indispensable to critical federal operations, including national defense, tax collection, import control, benefits payments, and law enforcement. Computers make it possible to process information quickly and communicate almost instantaneously among federal offices, outside organizations, and individuals. In addition, they make vast amounts of data accessible to anyone with a personal computer, a modem, and telephone.

However, this reliance on automated systems increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. The same factors that benefit operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on operations, possibly for purposes of fraud or sabotage or other malicious purposes. Threats of such actions are increasing, in part, because the number of individuals with computer skills is increasing and because intrusion, or "hacking," techniques have become readily accessible through magazines and on computer bulletin boards. In addition, natural disasters and inadvertent errors by authorized computer users can have devastating consequences if information resources are poorly protected.

¹Defending America's Cyberspace: National Plan for Information Systems Protection, Version 1.0, The White House, January 2000.

Recent audits show that federal systems are highly vulnerable to these risks. Our October 1999 analysis of our own and inspector general audits found that 22 of the largest federal agencies were not adequately protecting critical federal operations and assets from computer-based attacks.² Our most recent individual agency review, of the Environmental Protection Agency (EPA), corroborated our governmentwide analysis.³ Our tests identified numerous security weaknesses associated with the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations. In addition, EPA's own records identified several serious computer incidents in the last 2 years. EPA is currently taking significant steps to address these weaknesses, but resolving them on a lasting basis will require substantial ongoing management attention and changes in the way EPA views information security.

EPA is not unique. Within the past 12 months we have identified significant management weaknesses and control deficiencies at a number of agencies.

- In August 1999, we reported⁴ that pervasive weaknesses in Department of Defense information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data.
- In May 1999, we reported⁵ that as part of our tests of the National Aeronautics and Space Administration's (NASA) computer-based controls, we successfully penetrated several mission-critical systems, including one responsible for calculating detailed positioning data for each orbiting spacecraft and another that processes and distributes the scientific data received from these spacecraft. Having obtained access, we could have disrupted ongoing command and control operations and modified or destroyed system software and data.

²Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences (GAO/AIMD-00-1, October 1, 1999).

³Information Security: Fundamental Weaknesses Place EPA Data and Operations at Risk (GAO/T-AIMD-00-97, February 17, 2000).

⁴DOD Information Security: Serious Weaknesses Continue to Place Defense Operations at Risk (GAO/AIMD-99-107, August 26, 1999).

⁵Information Security: Many NASA Mission-Critical Systems Face Serious Risks (GAO/AIMD-99-47, May 20, 1999).

-
- In August 1999, an independent accounting firm reported⁶ that the Department of State's mainframe computers for domestic operations were vulnerable to unauthorized access. Consequently, other systems, which process data using these computers, could also be vulnerable. A year earlier, in May 1998, we reported⁷ that our tests at State demonstrated that its computer systems and the information they maintained were very susceptible to hackers, terrorists, or other unauthorized individuals seeking to damage State operations or reap financial gain by exploiting the department's information security weaknesses.
 - In October 1999, we reported⁸ that serious weaknesses placed sensitive information belonging to the Department of Veterans Affairs (VA) at risk of inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. Such findings were particularly troublesome since VA collects and maintains sensitive medical record and benefit payment information for veterans and family members and is responsible for tens of billions of dollars of benefit payments annually.

Control Weaknesses Are Similar Among Agencies

Although the nature of operations and related risks at these and other agencies vary, there are striking similarities in the specific types of weaknesses reported. The following six areas of management and general control weaknesses are repeatedly highlighted in our reviews.

- **Entitywide Security Program Planning and Management.** Each organization needs a set of management procedures and an organizational framework for identifying and assessing risks, deciding what policies and controls are needed, periodically evaluating the effectiveness of these policies and controls, and acting to address any identified weaknesses. These are the fundamental activities that allow an organization to manage its information security risks cost effectively, rather than reacting to individual problems ad hoc only after a violation has been detected or an audit finding has been reported. Despite the importance of this aspect of an information security program, we continue to find that poor security planning and management is the rule rather than the exception. Most

⁶*Audit of the Department of State's 1997 and 1998 Principal Financial Statements*, Leonard G. Birnbaum and Company, LLP, August 9, 1999.

⁷*Computer Security: Pervasive Serious Weaknesses Jeopardize State Department Operations* (GAO/ AIMD-98-145, May 18, 1998).

⁸*Information Systems: The Status of Computer Security at the Department of Veterans Affairs* (GAO/ AIMD-00-05, October 4, 1999).

agencies do not develop security plans for major systems based on risk, have not formally documented security policies, and have not implemented programs for testing and evaluating the effectiveness of the controls they rely on.

- **Access Controls.** Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. They include physical protections such as gates and guards. They also include logical controls, which are controls built into software that (1) require users to authenticate themselves through passwords or other identifiers and (2) limit the files and other resources that an authenticated user can access and the actions that he or she can execute. In many of our reviews we have found that managers do not identify or document access needs for individual users or groups, and, as a result, they provide overly broad access privileges to very large groups of users. Additionally, we often find that users share accounts and passwords or post passwords in plain view, making it impossible to trace specific transactions or modifications to an individual. Unfortunately, as a result of these and other access control weaknesses, auditors conducting penetration tests of agency systems are almost always successful in gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purposes they had in mind.
- **Application Software Development and Change Controls.** Application software development and change controls prevent unauthorized software programs or modifications to programs from being implemented. Without them, individuals can surreptitiously modify software programs to include processing steps or features that could later be exploited for personal gain or sabotage. In many of our audits, we find that (1) testing procedures are undisciplined and do not ensure that implemented software operates as intended, (2) implementation procedures do not ensure that only authorized software is used, and (3) access to software program libraries is inadequately controlled.
- **Segregation of Duties.** Segregation of duties refers to the policies, procedures, and organizational structure that help ensure that one individual cannot independently control all key aspects of a process or computer-related operation and thereby conduct unauthorized actions or gain unauthorized access to assets or records without detection. For example, one computer programmer should not be allowed to independently write, test, and approve program changes. We commonly find that computer programmers and operators are authorized to perform a wide variety of duties, thus providing them the ability to independently

modify, circumvent, and disable system security features. Similarly, we have also identified problems related to transaction processing, where all users of a financial management system can independently perform all of the steps needed to initiate and complete a payment.

- **System Software Controls.** System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation, e.g., operating systems, system utilities, security software, and database management systems. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate disclosures. Our reviews frequently identify systems with insufficiently restricted access that in turn makes it possible for knowledgeable individuals to disable or circumvent controls.
- **Service Continuity Controls.** Service continuity controls ensure that critical operations can continue when unexpected events occur, such as a temporary power failure, accidental loss of files, or even a major disaster such as a fire. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. At many of the agencies we have reviewed, we have found that plans and procedures are incomplete because operations and supporting resources had not been fully analyzed to determine which were most critical and would need to be restored first. In addition, disaster recovery plans are often not fully tested to identify their weaknesses. As a result, many agencies have inadequate assurance that they can recover operational capability in a timely, orderly manner after a disruptive attack.

Actions Agencies Can Take Immediately to Reduce Risks

Agencies can act immediately to address the weaknesses just described and thereby reduce the related risks. Specifically, they can (1) increase awareness, (2) ensure that existing controls are operating effectively, (3) ensure that software patches are up-to-date, (4) use automated scanning and testing tools to quickly identify problems, (5) propagate their best practices, and (6) ensure that their most common vulnerabilities are addressed. None of these actions alone will ensure good security. However, they take advantage of readily available information and tools and, thus, do not involve significant new resources. As a result, they are steps that can be made without delay. Let me briefly describe each of the actions I have mentioned.

Raise Awareness	<p>First, agency security managers can take steps to ensure that agency personnel at all levels understand the significance of their dependence on computer support and the related risks to mission-related operations. Better understanding risks allows senior executives to make more informed decisions regarding appropriate levels of financial and personnel resources to protect these assets over the long term. However, we have found that when senior managers do not understand such risks, they may not devote adequate resources to security or be willing to tolerate the inconvenience that may be associated with maintaining adequate controls. In addition, system users must understand the importance of complying with policies and controls and why these controls are important to the agency in meeting its mission-critical functions. Engendering such understanding and awareness requires a proactive approach from agency security experts and, most important, support from the agency head.</p>
Ensure Policies and Controls Are Operating Effectively	<p>Second, agencies should ensure that the policies and controls they have already implemented are operating as intended. Our audits often find that security is weak, not because agencies have no policies and controls, but because the policies and controls they have implemented are not operating effectively. In some cases they were never implemented appropriately. In other cases, the policies and controls have not been maintained. For example, assigning users password-controlled accounts on a system can be an effective way to help ensure that only authorized individuals gain access to the system. However, this control is significantly diminished if individuals who have retired, resigned, or otherwise left the agency retain access because system administrators have neglected to delete their accounts. To ensure that policies and controls are operating as intended, agencies must take steps to examine or test key controls routinely and enforce compliance with policies.</p>
Implement Software Patches	<p>Third, agencies should ensure that known software vulnerabilities are reduced by promptly implementing software patches. Security weaknesses are frequently discovered in commercial software packages after the software has been sold and implemented. To remedy these problems, vendors issue software "patches" that users of the software can install. In addition, organizations such as Carnegie Mellon University's CERT Coordination Center⁹ routinely issue alerts on software problems.</p>

⁹Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.

However, our audits have found that such patches are often not installed promptly or not installed at all, thereby leaving serious and widely known vulnerabilities open to exploitation. To avoid this situation, agencies must establish procedures for routinely (1) keeping system administrators aware of the latest software vulnerability alerts and the related remedial actions that need to be taken and (2) ensuring that needed patches are implemented promptly.

Routinely Use Automated Tools to Monitor Security

Fourth, agencies can use readily available software tools to help ensure that controls are operating as intended and that their systems are secure. Examples of such tools are (1) scanners that automatically search for system vulnerabilities, (2) password cracking tools, which test password strength, and (3) network monitoring tools, which can be used to monitor system configurations and network traffic, help identify unauthorized changes, and identify unusual or suspicious network activity. Such tools provide an efficient way to monitor system security, and their use is increasingly viewed as an essential aspect of good security practice, especially when they are used as part of a comprehensive security self-assessment program. However, tool use must be carefully managed to ensure that tools are not misused and that they lead to meaningful improvement. If not properly managed, using them could slow system performance. Similarly, results must be carefully analyzed to determine which identified problems are the most significant and whether and how they can be remedied. Placing tool selection, use, and related training under the control of a central security group can help ensure that tools are used appropriately and effectively throughout the agency. Central analysis of scanning results can also facilitate identification of appropriate safeguards and assist the agency in better understanding its risks.

Identify and Propagate Pockets of Excellence

Fifth, agencies can expand on the good practices that they already have in place. Our audits have shown that even agencies with poor security programs often have good practices in certain areas of their security programs or certain organizational units. In these cases, we recommend that the agency expand or build on the practice throughout the agency. For example, one unit in one agency we recently audited had developed strong intrusion detection capabilities, but this capability was not being developed in other units of the agency. Once again, central coordination can help identify these pockets of excellence and ensure that their value is maximized on an agencywide basis.

**Focus on the Most
Common Vulnerabilities
First**

Finally, agencies can develop and distribute lists of the most common types of vulnerabilities, accompanied by suggested corrective actions, so that individual organizational units can take advantage of experience gained by others. Such lists can be developed based on in-house experience, or agencies can adapt lists available through professional organizations and other centers of expertise. In the course of our audits, we frequently find the same vulnerabilities over and over again. By encouraging managers to monitor for the most common vulnerabilities continually, agencies can help ensure that they are promptly addressed, thereby quickly reducing their risk and possibly freeing technical experts to identify and address more difficult problems.

**Improved Security
Program Management
Is Essential**

While the actions I have just outlined can jump-start agency security improvement efforts, they will not result in fully effective and lasting improvements unless they are supported by a strong management framework. Such a framework can ensure that

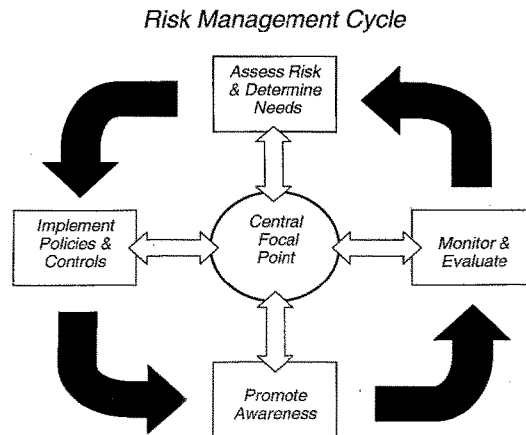
- agency actions are appropriately controlled and coordinated,
- testing tools are appropriately selected and tested prior to their use,
- personnel involved in using tools and in implementing software patches are properly trained,
- good practices and lessons learned are shared on an agencywide basis,
- controls are systematically tested to ensure that they are effective, and
- appropriate risk management decisions are made regarding the best way to address identified problems.

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

- assessing risks and determining protection needs,

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

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



This cycle of activity, as described in our May 1988 executive guide, is consistent with guidance on information security program management provide to agencies by the Office of Management and Budget (OMB) and by the National Institute of Standards and Technology (NIST). In addition, the guide has been endorsed by the federal Chief Information Officers (CIO) Council as a useful resource for agency managers. We believe that implementing such a cycle of activity is the key to ensuring that information security risks are adequately considered and addressed on an ongoing basis.

Need for New Governmentwide Actions to Support Agency Security Efforts

While individual agencies bear primary responsibility for the information security associated with their own operations and assets, there are several areas where governmentwide criteria and requirements could be strengthened. Existing requirements are somewhat out-of-date and do not provide agencies adequate guidance as to what levels of security are appropriate for their varying computer-supported operations. In addition, while the rigor and scope of our information security audits have increased in recent years, information on agency performance in this area is incomplete making it difficult to measure incremental improvements.

Perhaps most important, the legal framework supporting federal computer security needs to be updated. In particular, the Computer Security Act of 1987 is outmoded and inadequate, as well as poorly implemented. The act focuses too much attention on individual system security rather than requiring the agencywide perspective needed for today's networked environments. In addition, the act oversimplifies risk considerations by implying that there are only two categories of information: sensitive versus nonsensitive or classified versus nonclassified. As a result, it fails to recognize that security must be managed for a range of varying levels of risk to the integrity, availability, and confidentiality of information supporting agency operations and assets. Further, the act treats information security as a technical function rather than as a management function, which removes security from its integral role in program management. Lastly, the Computer Security Act does not require an evaluation of implemented controls (i.e., no testing). These deficiencies in the current legal framework lead directly to three specific areas where we believe governmentwide improvements are needed.

First, there is a need for routine periodic independent audits to provide (1) a basis for measuring agency performance and (2) information for strengthened oversight. Except for security audits associated with financial statement audits, current information security reviews are performed on an ad hoc basis.

Second, agencies need more prescriptive guidance regarding level of protection that is appropriate of their systems. Currently, agencies have wide discretion in deciding what computer security controls to implement and the level of rigor with which they enforce these controls. OMB and NIST guidance is not detailed enough to ensure that agencies are making appropriate judgments in this area and that they are protecting the same types of data consistently throughout the federal community. More specific guidance could be developed in two parts:

- A set of data classifications that could be used by all federal agencies to categorize the criticality and sensitivity of the data they generate and maintain. These classifications could range from noncritical, publicly available information requiring a relatively low level of protection to highly sensitive and critical information that requires an extremely high level of protection. Intermediate classifications could cover a range of financial and other important and sensitive data that require significant protection but not at the very highest levels. It would be important for these data classifications to be clearly defined and accompanied by guidelines regarding the types of data that would fall into each classification.
- A set of minimum mandatory control requirements for each classification. Such control requirements could cover issues such as (1) the strength of system user authentication techniques (e.g., passwords, smart cards, and biometrics) for each classification, (2) appropriate types of cryptographic tools for each classification, and (3) the frequency and rigor of testing appropriate for each classification.

Third, there is a need for stronger central leadership and coordination of information security-related activities across government. Under current law, responsibility for guidance and oversight of agency information security is divided among a number of agencies, including OMB, NIST, the General Services Administration, and the National Security Agency. Other organizations are also becoming involved through the administration's critical infrastructure protection initiative, including the Department of Justice and the Critical Infrastructure Assurance Office. The federal CIO Council is also supporting these efforts. While all of these organizations have made positive contributions, some roles and responsibilities are not clear and central coordination is lacking in certain key areas. In particular, information on vulnerabilities and related solutions is not being adequately shared among agencies and requirements related to handling and reporting security incidents are not clear.

In conclusion, I want to emphasize that while there are many valuable tools and practices that agencies can adopt, there is no "silver bullet" for information security. Ensuring effective and efficient progress in this area throughout the federal government will require concerted efforts by senior executives, program managers, and technical specialists. It will require cooperative efforts by executive agencies and by the central management agencies, such as OMB. Further, it will require sustained congressional oversight to ensure that improvements are realized.

Mr. Chairman, this concludes my statement. I would be happy to answer any questions you or other subcommittee members may have. For future contacts regarding this testimony, please contact me at (202) 512-6240.

Ordering Information

Orders by Internet

For information on how to access GAO reports on the Internet, send an e-mail message with "info" in the body to:

Info@www.gao.gov

or visit GAO's World Wide Web home page at:

<http://www.gao.gov>

**To Report Fraud,
Waste, and Abuse in
Federal Programs**

Contact one:

Web site: <http://www.gao.gov/fraudnet/fraudnet.htm>

E-mail: fraudnet@gao.gov

1-800-424-5454 (automated answering system)

Mr. HORN. I might add, I mentioned that all of your texts will be in when we introduce you. So will your resumes.

The next gentleman, the next two, have very rich resumes. Dr. David Nelson in particular has certainly been through the whole computer community, I can see, in terms of committees and responsibilities you have had.

Currently, he is Deputy Chief Information Officer at the National Aeronautics and Space Administration.

Mr. Nelson.

STATEMENT OF DAVE NELSON, DEPUTY CHIEF INFORMATION OFFICER, NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Mr. NELSON. Thank you, Mr. Chairman. Members of the subcommittee, I am pleased to appear before you today to discuss NASA's views on the security of our information technology environment. I have submitted my written statement for the record. My oral summary will be quite consistent with that of Mr. Brock.

I would like to emphasize three points. My first point is the importance of a sound management framework for information technology security. Two years ago, NASA did not have a satisfactory framework. Since then we have worked hard to align our policy, organization, funding and objectives for effective security.

This began with senior management attention and support, including the recognition that information technology security is required for safety of lives and property. In an internal study, we benchmarked ourselves against good organizations and copied the best of what we found. We accepted the recommendations of the General Accounting Office review of NASA security that Mr. Brock referred to.

Our actions included issuing up-to-date policy, establishing a senior Council to set strategic directions, clarifying management responsibilities, budgeting for key tasks and collecting metrics of progress.

NASA places operational responsibility for information technology security on line management, complemented by a cadre of computer security professionals who provide technical assistance and oversight.

I have mentioned budgets and metrics. If I could have the chart, please.

This chart shows one of our metrics. Plotted is the number of serious incidents. Those are things like destruction of data, theft of passwords, or damage to software, versus on the X axis the percent of the information technology budget that is spent on security. Each point is a specific center, and the data is real. Notice the trend line. As you start from the left, as the percentage of budget increases to about 2 percent, the number of incidents levels off. This suggests that spending about 2 percent of information technology budget on security gives a good return on information. Spending less increases risk, as shown by the trend line. Spending more may not add much return. We have compared notes on this metric with leading companies. They see the same sort of trend and the same sort of sweet spot.

Now, this metric isn't perfect, but it gives us a place to start. Metrics like this are our headlights. They guide our actions and indicate where we need to work harder.

My second point is the importance of training. NASA is a highly technical organization. We create and modify leading-edge information systems to serve our missions. Security risk evolves as threats and, as a result, vulnerabilities change, so our personnel must understand the principles of effective security and apply them to changing situations. Program and project managers must be trained to evaluate risks and vulnerabilities in designing and maintaining systems entrusted to them. System administrators must be trained to properly configure and upgrade their systems, to recognize attacks and to respond to them. Users must be trained to practice good security, to recognize certain types of attack, and to know how to get help.

Over the last 2 years, NASA has developed or acquired new training material for managers, system administrators, and users. This training is now mandatory for all civil servants, and we are gathering metrics on its delivery. In addition, NASA has requested comments on a draft regulation that would require NASA contractors to adhere to the same standards of training that apply to civil servants.

My last point is the importance of appropriate tools. Security tools, which are a combination of computer hardware and software programs, help to protect systems and defend against attacks.

The technical details of a particular attack may be very complicated, but once the attack is understood, defense against it can be incorporated into a tool that is easy to use by a trained person.

Organizations with modest funding, but substantial technical skills can obtain free, reputable tools from the Internet that offer good capability. However, they may not be well-documented or supported and may be somewhat difficult to use. NASA tends to purchase key commercial tools and augment them with free tools. Obviously, purchased commercial tools have a higher initial cost. However, they are often easier to use and may have a lower sustaining labor cost.

Most successful attacks are enabled by a relatively small number of weaknesses, as Mr. Brock has observed. These include lack of virus detection software; trivial passwords that can easily be cracked, that means decrypted; failures to install patches for well-known software vulnerabilities; and poorly configured computers with open vulnerability holes. Tools help us to deal with each of these classes of problems. In my written statement, I have described a number of these and the practices that NASA uses.

New problems keep appearing, along with new defenses. Thus, the tools and their use must evolve. There is no substitute for good proactive management that can respond quickly and effectively. Unfortunately, easy-to-use tools for attacking systems are also available on the Internet, and they are constantly getting better. This means it takes less skill to mount a sophisticated attack than it used to. The ecologists would call this a classic predator-prey situation in which both predator and prey evolve quickly to secure competitive advantage.

In conclusion, NASA is facing the challenge of the evolving security universe by marshalling effective management, effective training, and effective technology. We are in an environment of increasingly numerous and serious threats, along with systems whose vulnerabilities tend to increase as they become more complicated.

Fortunately, our tools and process allow us to make progress in dealing with this environment, but it is a never-ending process. We take response—we take seriously our responsibility as stewards of the public's space and aeronautics information and systems. We are committed to working with other agencies of the executive branch and with the Congress to ensure that we maintain the proper balance between accessibility of research results and protection of our information technology investment.

Thank you for the opportunity to testify before you today. I look forward to answering your questions.

Mr. HORN. Well, thank you very much.

[The prepared statement of Mr. Nelson follows.]



National Aeronautics and
Space Administration

Hold for Release Until
Presented by Witness

March 29, 2000

Subcommittee on Government Management, Information, and Technology

Committee on Government Reform

House of Representatives

Statement by:
David Nelson
Deputy Chief Information Officer
Office of the Administrator

Statement of
David B. Nelson
Deputy Chief Information Officer
National Aeronautics and Space Administration

before the

Subcommittee on Government Management, Information, and Technology
Committee on Government Reform
House of Representatives

Mr. Chairman and Members of the Subcommittee:

I am pleased to appear before the Subcommittee today to discuss with you NASA's views on the security of our information technology (IT) environment. As Deputy Chief Information Officer, I have overall responsibility for NASA's unclassified information technology security, under the Chief Information Officer (CIO).

NASA faces substantial challenges in providing a secure environment for our missions, while fulfilling our statutory requirement to share information with the public and to collaborate with academia and the private sector. NASA's budget for IT is about \$2.1 billion; we have over sixteen thousand host computers (not including desktop computers); we move one million E-mail messages per day; and NASA.gov has been rated the highest volume Government Website by Media Metrix. Our use of the Internet presents particularly significant and rapidly changing risks. However, we see so many benefits arising from use of the Internet that our task is to manage these risks rather than avoid them. Our challenge is rendered more difficult because the Internet was not designed for high security. Neither was much of our key software, including operating systems and core applications. And as a technical agency, NASA is constantly pushing the state of the art in computing and networking, requiring us to use ever more advanced security techniques and products.

Concurrently, the number and seriousness of attacks on NASA computer systems are growing. Our metrics show increasing success in detecting and deflecting these attacks, but we are still not where we want to be. Two years ago, the pressing need for improved IT security was made clear by our internal security study; audits by the General Accounting Office and an independent financial auditor; and audits, reviews and inspections by the NASA Inspector General. As a result, we significantly changed our IT security approach. I believe a description of this approach may be helpful to other Federal Agencies facing similar challenges.

Security Framework

Despite the highly technical nature of IT security, its effectiveness is governed by standard management principles. Without good management, even the best technology will not be effectively deployed and used in a large organization such as NASA.

Leadership

The most important factor in IT security is senior management leadership and support. Fortunately, NASA management provides that leadership, consistently and publicly. Last May the NASA Administrator issued a message to all Agency management for distribution to all personnel, emphasizing the importance of ensuring that our computer systems and data are safe and secure. His message included the following statement:

“As with all aspects of safety—our success in ensuring the security and integrity of NASA computing resources and data begins and ends with you. Each of your employees plays a critical role in ensuring the overall level of integrity, confidentiality, and availability of information and information systems. Take it seriously.”

NASA’s CIO and I have personally delivered awareness and training briefings to all senior and middle management at all NASA Centers, as part of the Administrator’s Security Campaign.

To ensure understanding and support by Enterprise senior management, NASA has established an IT Security Council. This Council provides top level guidance on strategy and investment. NASA places operational responsibility for IT security on line management, complemented by a cadre of computer security professionals who provide technical assistance and oversight.

Funding

As a result of management support, NASA has been able to fund the most critical security acquisitions and operations. We gather data on current and proposed costs as part of our internal budget process, and IT security issues are explicitly considered as part of Agency budget formulation. We have had to prioritize carefully, and this effort has at times proven difficult, but I believe we now have sufficient resources to achieve our goals. By comparing Center-level funding of IT security with measures of security effectiveness, we have found that devoting roughly two percent of IT funding to IT security provides adequate resources. Our finding is consistent with that reported by leading companies. We continue to test the validity of this metric in annual data collections.

Management

Information technology security is led by the Agency CIO Office, within the Office of the Administrator. The program is managed as a partnership between the CIO and line management. The CIO Office establishes policy, defines Agency-level training criteria, defines and funds most common investments, and assesses the effectiveness of the IT security program by gathering and analyzing metrics. We have devoted considerable

effort to issuing uniform policies and procedures, derived from OMB Circular A-130, so that everyone knows what is expected. The Office of Human Resources and Education partners with the NASA CIO in curriculum development and delivery of training for civil servants. Enterprises are responsible for ensuring that IT security is an integral part of institutional, program, and project management. Center Directors, working through Center CIO's, are responsible for operation and maintenance of IT investments, as well as implementation of IT security training of civil servants and contractors (i.e., incorporation into contracts). They are also responsible for ensuring that both employees and contractors adhere to IT Security policies and procedures and are held accountable for failure to do so. Furthermore, all parties must ensure that all funding requirements are specified and defended, as required by the rules governing NASA's budget process.

Training

NASA is a highly technical organization that is constantly creating and modifying leading-edge information systems to serve its missions. Training is essential for managers, engineers, and technicians to design and maintain adequate IT security in systems entrusted to them. Besides being good practice, Federal laws mandate periodic training in IT security awareness and IT security practices for all employees that use, manage, or design systems. This requirement includes IT security and risk management training for all program and project managers. However, both the GAO audit and the internal IT Security Program Review found that NASA IT security training practices were inadequate and inconsistent.

Since then, we have greatly strengthened our training for users, managers, and system administrators. In cooperation with the Defense Information Systems Agency, NASA has produced an award-winning CD-ROM-based IT security awareness training course, which has been distributed to all Agency Centers. We have adapted this training to Web delivery and have added manager awareness and manager risk assessment training. NASA is also piloting intensive training for system administrators in several Centers. In addition, the Agency has requested comment on a draft regulation that would require NASA contractors to adhere to the same standards of training that apply to civil servants. Finally, a metric has been established, under the Government Performance and Results Act (GPRA), specifying that at least eighty percent of our civil service users and managers will be trained by the end of this fiscal year.

Technical Operations

The NASA CIO has established a Principal Center for IT security at the Ames Research Center (ARC), led by a manager who reports to the CIO and the Center Director. The Principal Center manager ensures a close working relationship among the CIO, the Enterprises, and the Centers regarding IT security. The manager is responsible for recommending information security policies, procedures, guidance, architecture, standards, and metrics. This responsibility fits well with ARC's role as the NASA Center of Excellence in IT. ARC, located in Silicon Valley, is ideally situated to facilitate the infusion of new computer and communications security technology and products to meet

near-term and long-term NASA requirements. In order to better leverage the wealth of expertise that resides across NASA's Centers, we have also established Expert Centers in IT security, coordinated by ARC, with assigned functional responsibilities. The functional areas and associated Expert Centers are:

- Notifications, Incident Coordination, and Response - Goddard Space Flight Center;
- Training and Awareness - Glenn Research Center;
- Networking and Communications - Marshall Space Flight Center;
- System Auditing and Monitoring - Jet Propulsion Laboratory; and
- Technology Development - ARC.

At all of NASA's Research Centers, the oversight responsibilities for IT security are exercised by the IT security manager and the Center CIO, with the IT security manager often reporting to the CIO. In any case, we are working to ensure that their relationship is close and productive. The IT security manager and CIO review security plans and operations and create a web of information flow, reaching out to network operations personnel and systems administrators and providing technical assistance to line management.

We require that all computer incidents, defined in NASA policies, be reported to the IT security manager and then to the NASA Automated Systems Incident Response Capability (NASIRC) located at Goddard Space Flight Center. Information concerning any criminal attacks is forwarded to NASA's Inspector General for investigation. NASIRC distributes alerts of attacks, analyzes attack patterns, distributes bulletins of vulnerabilities and fixes, and collects metrics of incidents. We analyze these metrics to understand the nature and frequency of attacks and the success of our defenses.

NASA has executed a memorandum of cooperation between NASIRC and the Federal Computer Incident Response Capability located in the General Services Administration. We work closely with alert services such as the Computer Emergency Response Team at Carnegie Mellon University and other international response teams and monitor vendor notices and news groups. IT Security is a worldwide issue, especially for those who have extensive Internet connectivity. By actively facilitating coordination and collaboration with other organizations around the world, we are able to obtain timely "heads-up" information to better protect our IT system environments. We can also share lessons learned with others who are working on similar issues, in an atmosphere of trust and mutual support. With the increase in our use of portable computers, NASA is implementing technology that assists us in deterring theft and recovering our hardware and information if computers are stolen.

Readily Available Tools

Most successful attacks on NASA systems are enabled by a relatively small number of IT security weaknesses. These include:

- lack of virus detection software;
- trivial passwords that can easily be "cracked";

- failure to install “patches” for well-known software vulnerabilities; and
- poorly configured computers with open vulnerability holes.

We defend against such weaknesses through a combination of measures that provide a defense-in-depth. These measures include proper design and configuration, as well as the use of specific tools to sense and respond to attacks. NASA tends to purchase key commercial tools and then augment them with open-source tools. Obviously, purchased commercial tools have a higher initial cost. However, they are also often easier to use and therefore have a lower sustaining labor cost.

Firewalls

Firewalls restrict the passage of network traffic into a facility, according to rules set by the network administrator. Properly used, they provide a degree of protection for computers inside the facility. All of our Centers use firewalls, but we do not consider these to be a panacea, because firewalls can be compromised and bypassed. Furthermore, they cannot deal with very high-speed data, and some applications require that a firewall allow passage of types of data that are “risky.” NASA has issued a technical standard for firewall capabilities and a “trust model” for firewall rule sets that provide a common level of defense at each of our ten Center borders. Firewalls are also used for within-Center enclaves requiring a higher level of security. Most of the firewalls used by NASA are commercial products.

System Scanning Tools

System scanning tools audit computers by accessing them through their network connection. Usually they are installed inside any firewall so as to have complete access to our computers and networks. They can identify risky configurations and test for some software vulnerabilities. We have installed a common set of scanning tools at all Centers and are using them to scan for the “top fifty” vulnerabilities that have been identified as common to NASA systems, as well as other serious vulnerabilities that are discovered. Any vulnerabilities are reported to local management, and the affected systems are rescanned to verify compliance. NASA will be informing Congress of our success in reducing these vulnerabilities, as part of our general GPRM metrics reporting process.

A variant of the system scanning tool is the network mapping tool. This is used to determine the topology of a network and to identify systems attached to it. We have used this tool to map out networks that are not well documented.

Intrusion Detection Tools

Intrusion detection tools watch network traffic for signs of an attack. They are programmed with traffic patterns characteristic of known attacks. When a known pattern is matched, they send an alert to the administrator. We have installed a common set of intrusion detection tools at all Centers. Today, analysis of intrusion detection is largely manual and labor intensive, but we are looking at techniques to assemble data from all Centers for more automated analysis and reporting.

Sniffer Tools

Sniffers are similar to intrusion detection tools. They watch network traffic for interesting information. Used by network managers, they provide information on network congestion or other operational issues. Used by attackers, they provide user names and passwords for computers on the network. Attackers will often attack and seize one computer on a network, install a software sniffer, and grab user names and passwords to attack other computers.

Password Cracking Tools

Password cracking tools attempt to determine user passwords by decrypting (i.e., cracking) the encrypted password files stored on computers. Attackers use these tools to gain access to user accounts. We use them to audit whether trivial passwords are being used. Unfortunately, these tools can now crack passwords that were once considered strong, requiring a move to more complicated passwords that are harder to remember. NASA standard calls for at least eight character passwords containing a mix of alpha-numeric characters. We enforce this standard using software that examines a newly-entered password and rejects it if it is not strong enough. In the future, we and other organizations will need to move to stronger methods of authentication.

Strong Authentication

The problems of passwords have caused a move towards strong authentication, which uses a mixture of features (e.g., typically “something you have, and something you know”). An example is a portable hardware device that generates a new number every minute (something you have), augmented by a password (something you know). Login requires both the generated number and the password. The host computer knows the number generated by the hardware device and can verify that the number and password are correct. If the number and password combination are intercepted, they are not usable later. If the hardware device is stolen, it is useless without the correct password. NASA already uses these hardware devices in some Centers. Other examples of strong authentication include public key certificates and bio-metric devices.

Public Key Infrastructure

Public key tools provide authentication and encryption services and are a form of strong authentication. They are managed using an infrastructure that ensures reliability and broad scope. NASA has procured and is deploying public key tools to all employees. We are a member of the Federal Public Key Infrastructure Steering Committee and are participating in the public key bridge authority being established by the committee.

Availability of Tools

In addition to commercial sources, many of the tool types discussed above are freely available on the Internet. NASIRC maintains a repository of the tools that is accessible through the Website www.nasirc.nasa.gov. Another source for these tools is the Computer Emergency Response Team whose Website is at www.cert.org.

Conclusion

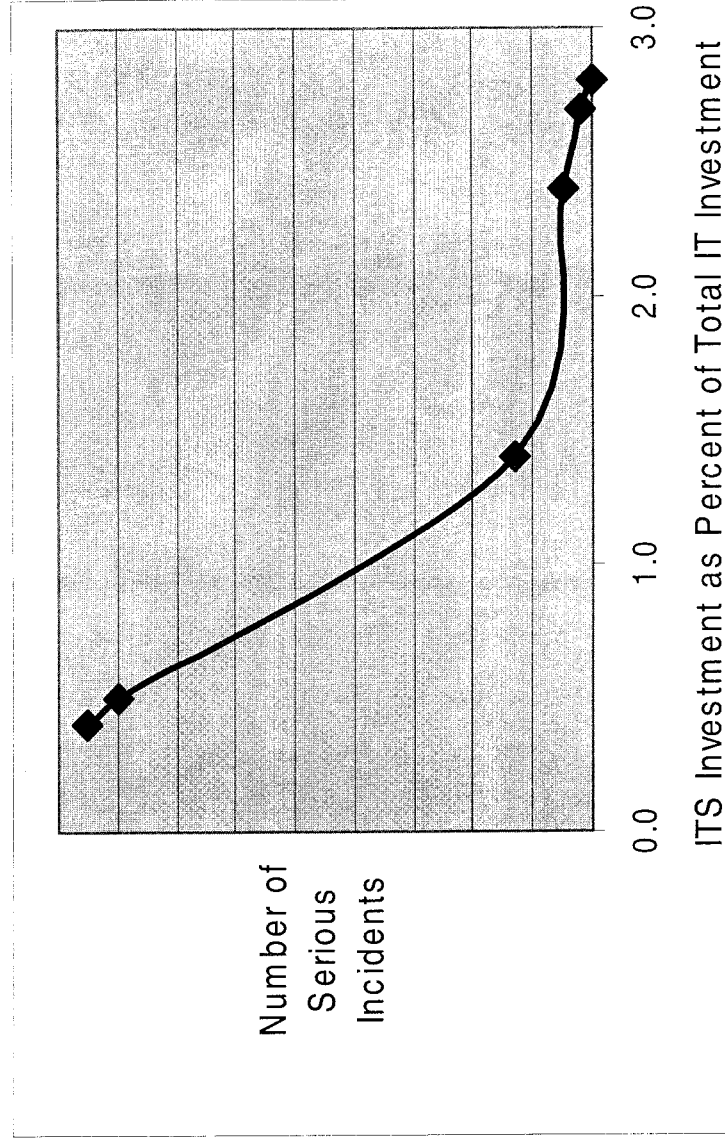
NASA is facing the challenge of the evolving IT universe by marshalling both effective management and effective technology. Information sharing is essential to achieve the mission of NASA. NASA not only has a strong presence on the Internet, but also must maintain separate and protected mission critical information technology systems. As a direct result of our very strong presence on the Internet, we have become a significant player in the incident-handling arena that cuts across both civilian and military Government entities, private industry, academia, and our foreign partners.

We face an environment of increasingly numerous and challenging threats, along with systems whose vulnerabilities tend to increase as they become more complicated. Fortunately our tools and processes allow us to make progress in dealing with this environment. Our metrics are very important, for they are like our "headlights." They guide our actions and indicate where we need to work harder. We are not yet where we want to be in protecting our resources, while retaining our openness to the public. However, we have some confidence that we are getting there.

In summary, we take seriously our responsibility as stewards of the public's space and aeronautics information systems. We are committed to working with other Agencies of the Executive Branch and with the Congress to ensure that we maintain the proper balance between accessibility of research results and protection of our IT investment.

Thank you for the opportunity to testify before you today. I look forward to answering your questions.

Attacks on NASA Systems



Mr. HORN. Those bells show that there is a vote on the floor, so we are going to have to go into recess for 20 minutes before we will take up Mr. Collier and then the questions. So relax.

[Recess.]

Mr. HORN. The subcommittee will now end the recess for the voting on the floor, and we will begin with Mr. Paul Collier, division general manager of Identix Solutions.

You might want to tell us a little about Identix Solutions. Put in a plug so I can understand it.

Go ahead, Mr. Collier.

**STATEMENT OF PAUL COLLIER, DIVISION GENERAL
MANAGER, IDENTIX, INC.**

Mr. COLLIER. Thank you, Mr. Chairman. Thank you for inviting me to be a part of this distinguished panel today. My testimony will focus on technology available that offers a significant advance in the protection of computer networks and critical data systems.

The greatest challenge we face in controlling access to computers and information is positive user authentication. Recent events show that the proliferation of the Internet, our increased reliance on computer-based information and the rapid growth of mobile computing has far outpaced our ability to secure these systems.

Traditionally the use of passwords has been our best defense. Recent advances in password cracking software and increased computer processor speeds have required passwords to become more complex and changed more frequently.

The human element in this new equation has been pushed to the limit. We now see more passwords written on the back of mouse pads, on desk leaves, and even on Post-It notes affixed to monitors. In addition, users tend to leave work stations logged on and unattended because of the added inconvenience.

It should be noted that there is no single technology that can serve as a panacea for positive user authentication. However, a combination of available technologies, working in concert, can provide a significant advance in addressing this need. The positive user authentication model consists of three elements, something you have, something you know, and something you are: Something you have, such as a smart card with a digital certificate embedded in the microprocessor; something you know, a simple PIN, as few as four digits; and something you are, one or more biometrics.

Someone can give an unauthorized individual their smart card or token and tell them their PIN number or password. The biometric is the only nontransferable element in this model. Briefly, a biometric is a quantitative measurement of a unique human attribute or behavioral characteristic, such as fingerprints, face, voice, iris pattern, etc.

Using fingerprints as an example in this model, a finger is placed on a sensor and then scanned. The image of the fingerprint is then processed by a series of algorithms which convert it into a binary representation or template. This template is then compared to a reference template stored either on a computer or a card-based data storage medium. Like most biometrics, you cannot reverse-engineer this binary representation and recreate the fingerprint image.

Fingerprint biometrics have been used in many civil and government programs for over 10 years. They have been very effective in reducing fraud, eliminating multiple identities, and securing access to sensitive areas.

These wide-scale deployments have served as real-world proving grounds for this technology and involve many millions of people. Knowledge gained from these programs and applied to improvements and cost reductions help produce much of the commercial products available today.

The Federal Government, in partnership with industry, has made a significant contribution to the evolution of biometric technology. Biometrics would not have advanced to their present level without the help of such agencies as the Department of Defense, the National Security Agency, the Departments of Justice, Energy, Treasury and the National Institute for Standards and Technology.

Like many technologies, biometrics have become faster, better, and cheaper. An example, only a few years ago the cost to integrate fingerprint biometric technology was approximately \$3,000 per computer. Recent advances have reduced the cost to less than \$100 per computer. History has shown the ephemeral nature of benchmarks in information technology, and in the near future we can anticipate still further reduction in costs and improved performance.

Commercial Off-The-Shelf products are entering the government market via GSA schedule and other procurement vehicles. The recent Smart Access/Common ID procurement by the General Services Administration represents a 10-year, \$1.5 billion government-wide contract that includes provisions for biometrics used for both physical and logical access.

Mr. Chairman, with your permission, I would like to demonstrate two of the products available today. The first is configured to demonstrate the positive user authentication model that I discussed earlier. The computer work station that you see here is in a locked mode. Attached to it is a keyboard with an integrated smart card reader and fingerprint scanner. These are commercially available, and the government has really taken to this particular one. The user takes his or her smart card, which, as you can see, has the smart card chip on the back, and inserts it into the work station. The log-on prompts the user to choose their log-on ID, enter the four-digit PIN number, which is the something-you-know portion—it is telling me I haven't put my finger on the scanner—and then place my finger on the scanner to complete the log-in process.

If the user removes the smart card from the computer keyboard, the system locks.

The second product, which is available commercially, many of the components of which were developed in conjunction with the National Security Agency, is a PC card which has a built-in fingerprint scanner. This is a simple replacement for password configuration that you see here. The user need only go up to the computer, place their finger on the scanner, and the log-on process is complete, nothing to remember.

In 1998, several key companies founded the International Biometrics Industry Association. The charter is a nonprofit trade association to promote competition, establish an industry code of ethics, represent industry concerns, and serve as a single voice on major

issues such as privacy, computer security, e-commerce, and legislative issues.

I would like to thank the chairman for the opportunity to appear here today and demonstrate these products to you. Thank you, Mr. Chairman.

Mr. HORN. Well, we thank you and your other two colleagues there.

[The prepared statement of Mr. Collier follows:]

Hearing before the
House Committee on Government Reform

Subcommittee on Government Management, Information
and Technology

March 29, 2000

Testimony of

M. Paul Collier
Division General Manager
Identix, Inc.

Mr. Chairman, members of the subcommittee, thank you for inviting me to be a part of this distinguished panel. My testimony will focus on technology available today that offers a significant advance in the protection of computer networks and critical data systems.

The greatest challenge we face in controlling access to computers and information is positive user authentication. Recent events show that the proliferation of the Internet, our increased reliance on computer-based information and the rapid growth of mobile computing have far outpaced our ability to secure these systems.

Traditionally, the use of passwords has been our best defense. Recent advances in password "cracking" software and increased computer processor speeds have required passwords to become more complex and changed more frequently. The human element in this new equation has been pushed to the limit. We now see more passwords written on the back of mouse pads, on desk leaves and even on post-it notes affixed to monitors. In addition, users tend to leave workstations logged-on and unattended because of the added inconvenience.

Current Authentication Issues

- Passwords can be forgotten, stolen, misused
- Password schemes are difficult for users
 - Industry:
 - Up to 50% of help desk calls are for forgotten or expiring password
 - Password changes every 60 days
 - Average cost to maintain a password user is \$145 per year

It should be noted that there is no single technology that can serve as a panacea for positive user authentication. However, a combination of available technologies working in concert can provide a significant advance in addressing this need. The positive user authentication model consists of three elements; something you have, something you know and something you are.

- Something you have: smart-card with digital certificate
- Something you know: a simple PIN
- Something you are: one, or more biometrics

Someone can give an unauthorized individual their smart card and tell them their PIN number or password. The biometric the only nontransferable element in this model.

A biometric is quantitative measurement of a unique human attribute or behavioral characteristic. These include:

Fingerprints	Thermal (Face)
Voice	Vein Patterns (Hand)
Facial	Finger Geometry
Iris	Stride Recognition
Retina	DNA
Signature Dynamics	Keystroke Dynamics
Hand Geometry	Body Odor

Using fingerprints as an example; a finger is placed on a sensor and then scanned. The image of the fingerprint is then processed by a series of algorithms, which convert it into a binary representation, or template. This template is then compared to a reference template stored either on a computer or card based data storage medium. Like most biometrics, you cannot reverse engineer this binary representation and recreate the fingerprint image.

- Minutiae-based algorithms have a rich history (20 years in Law Enforcement)
- Traditional measurements of the finger:
 - Ridge Endings
 - Bifurcation's

Fingerprint biometrics have been used in many civil and government programs for over ten years. They have been very effective in reducing fraud, eliminating multiple identities and securing access to sensitive areas. These wide-scale deployments have served as real world proving grounds for this technology and involved many millions of people. Knowledge gained from these programs and applied to improvements and cost reductions helped produce many of the commercial products available today.

Federal Deployment Examples

- DOD / RAPIDS & DEERS
- DOD / Operation Mongoose
- DOD / National Security Agency
- DOD / DMDC - BIDS
- US Department of the Treasury Electronic Money Project
- US Secret Service - Operation TRIP
- US Department of State (BCC)
- US Social Security Administration (OIA)
- FBI - WV Facility Access Control

Civil and Government Deployment Examples

- Spanish Social Security Program
- Georgia Driver's License
- West Virginia Driver's License
- Costa Rica Voter Registration
- Dominican Republic
- Panama
- San Diego Welfare Control
- New Delhi Driver's License
- El Salvador Driver's License
- United Nations HCR Refugee Tracking

The federal government, in partnership with industry has made a significant contribution to the evolution of biometric technology. Biometrics would not have advanced to their present level without the help of the Department of Defense, National Security Agency, Department's of Justice, Energy, Treasury and the National Institute for Standards and Technology.

Government and industry have worked together to develop necessary standards for technology integration and interoperability. Both the National Security Agency and the National Institute for Standards and Technology have initiated several of these efforts and have served as co-chairs of several activities.

Some of these standards activities include:

- BioAPI Consortium
- NIST Common Biometric Exchange File Format
- ANSI / NIST Standard for Fingerprint Data Interchange
- Biometric Consortium
- Association Motor Vehicle Administrators (AMVA)
- NSA/GSA X.509 Standard

In 1998, several key companies founded the International Biometrics Industry Association. The charter of this non-profit trade association is to promote competition, establish an industry code of ethics, represent industry concerns and serve as a single voice on major issues such as privacy, computer security, e-commerce and legislative issues.

Like many technologies, biometrics have become faster, better and cheaper. In example, only a few years ago the cost to integrate fingerprint biometric technology was approximately \$3,000 per computer. Recent advances have reduced the cost to less than \$100 per computer. History has shown the ephemeral nature of benchmarks in information technology. In the near future we can anticipate still further reduction in costs and improved performance.

Commercial-off-the-shelf-products are entering the government market via GSA schedule and other procurement vehicles. The recent Smart Access / Common ID procurement by the General Services Administration represents a ten year, \$1.5 billion government wide contract that includes provisions for biometrics used for both physical and logical access.

Mr. Chairman, with your permission I would like to demonstrate two of the products available today. The first is configured to demonstrate the positive user authentication model discussed earlier.

The first of these products is Biologon with BioCard:

- The computer workstation is in a locked mode.
- The user inserts his, or her smart-card in a reader integrated into the keyboard
- The logon process then prompts the user to enter a four digit PIN
- They are then prompted to place their finger on the integrated scanner
- The logon process is now complete
- If the user removes their smart-card from the reader, the computer logs off

Biologon Product Overview

- **MS Windows 2000/98/95/NT 4.0**
- Workstation, PDC, BDC
- Integrated into MS SAM
- Support Various Integrated Peripherals
- Enrollment Wizard
- Variable Thresholds
- Multiple Finger Enrollment
 - User / Administrator Friendly
 - Simplifies Logon Process
 - Decreases Cost of Network Ownership
 - Seamless Integration
 - Client/Server 3-5 MB
 - Biometric template size 256 bytes
- Security Pack
 - BioSafe
 - Encrypt/Decrypt files on Desktop using Standard RSA encryption algorithms
 - BioShield
 - Locks Applications
- BioCard Client
 - Enables Token Layer (Smart Card)

The second product is the BioTouch PC card:

- This product has been configured to demonstrate simple password replacement
- The BioTouch has been inserted in the PC card slot and the notebook is locked
- The user need only place an enrolled finger on the scanner to log-on

Thank you Mr. Chairman.

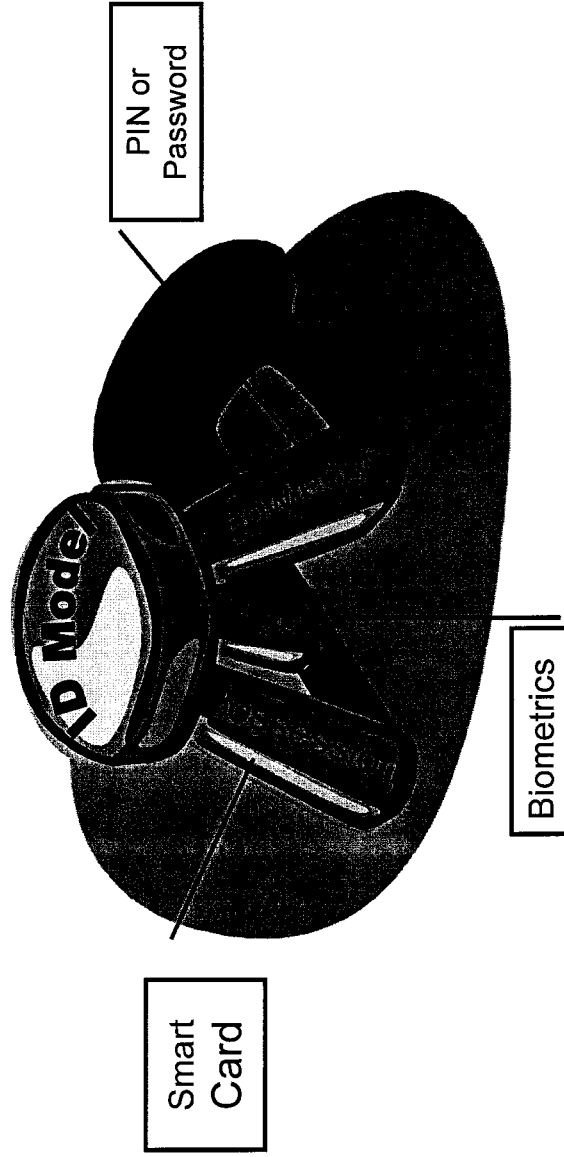
Biometrics in IT Security

U.S. House of Representatives
Committee on Government Reform
Subcommittee on Government Management,
Information and Technology

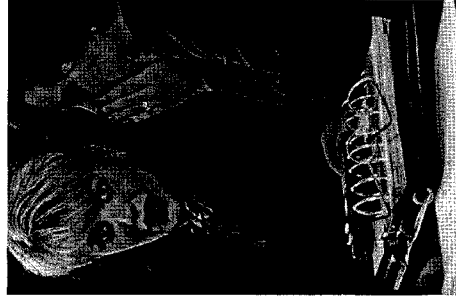
March 29, 2000

Positive User Authentication

© 2015 Intel Corporation. All rights reserved. Intel, the Intel logo, and Intel Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries. Other brands and product names are trademarks of their respective owners.



PINs and Passwords are Transferable



Pssst... I can tell you
my PIN or password,
but can't give you my
fingerprint!

Biometric Technology (Methods)

- Fingerprints
- Voice
- Facial
- Iris
- Retina
- Signature Dynamics
- Hand Geometry
- Thermal (Face)
- Vein Patterns (Hand)
- Finger Geometry
- Stride Recognition
- DNA
- Keystroke Dynamics
- Body Odor

Technology

- Minutiae-based algorithms have a rich history (20 years in Law Enforcement)
 - Traditional measurements of the finger:
 - Ridge Endings
 - Bifurcation's
 - Identicator's Eight Measurements

Core Location Directions
Vector to Minutiae Ridge Count
Minutiae Direction
Minutiae Coordinates
Coordinate System



The Technology

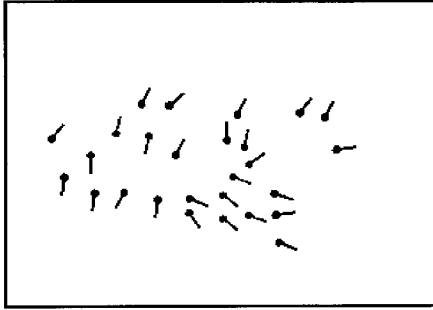
53



Finger Image



Finger Image +
Minutiae

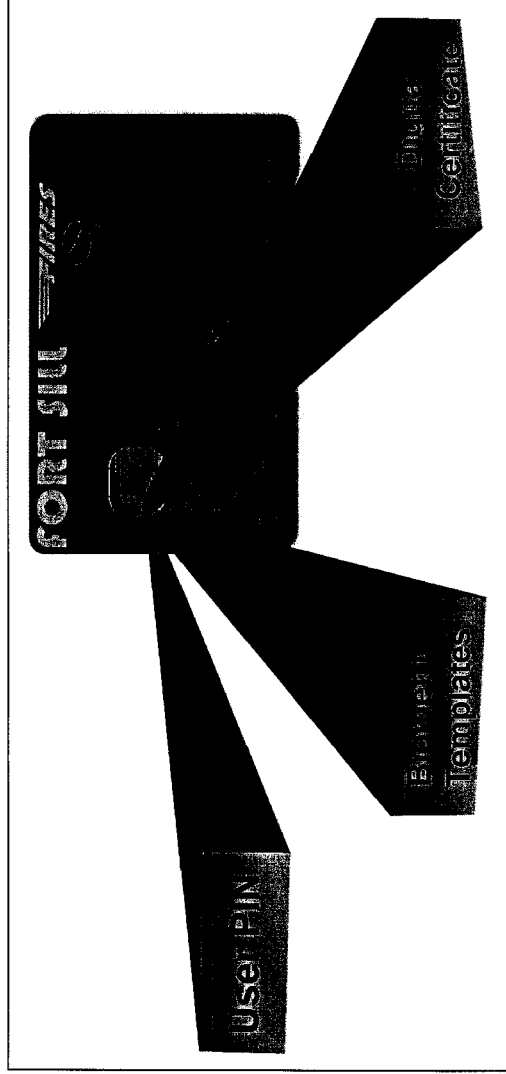


Minutiae

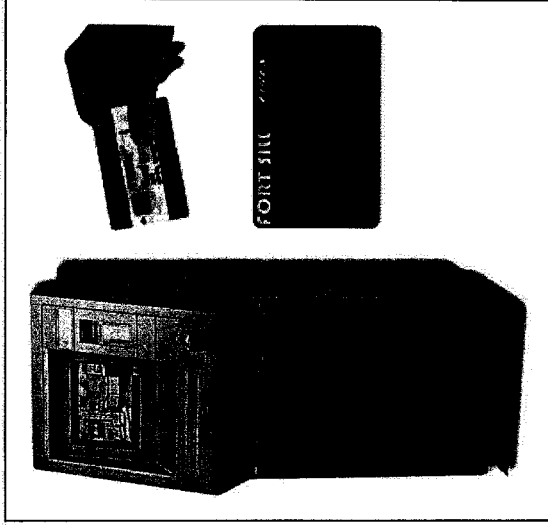
identix

Biometrics, PKI and Smart Cards

Source: <http://www.fortiss.com/Products/SmartCards/SmartCards.htm>



Deployment



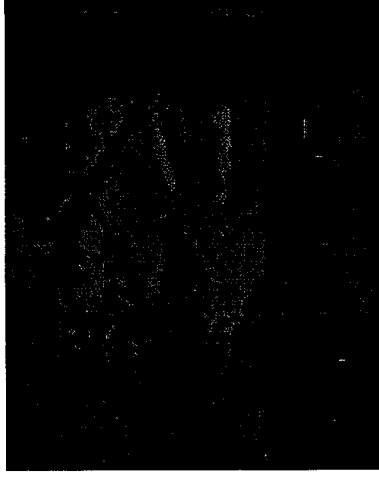
- **Government Project Background:**

- Spanish Social Security Program
 - (UNISYS)
- Georgia Driver's License
 - (Polaroid)
- West Virginia Driver's License
 - (Polaroid)
- Costa Rica Voter Registration
- Dominican Republic
- Panama
 - (UNISYS)
- San Diego Welfare Control
 - (UNISYS)
- New Delhi Driver's License
 - (HCL)
- El Salvador Driver's License
 - (Talsud)
- United Nations HCR Refugee Tracking

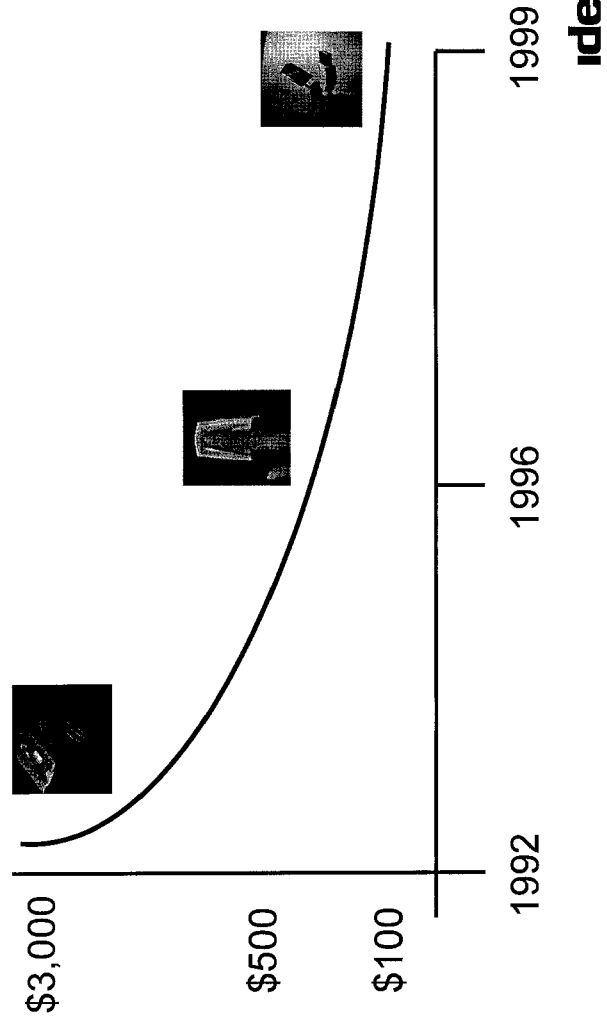
identix

Deployment

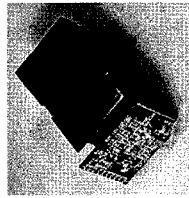
- Federal Government Project
Background:
 - DOD / RAPIDS & DEERS
 - DOD / Operation Mongoose
 - DOD / National Security Agency
 - DOD / DMDC - BIDS
 - US Department of the Treasury
Electronic Money Project
 - US Secret Service - Operation
TRIP
 - US Department of State (BCC)
 - US Social Security
Administration (OIA)
 - FBI - WV Facility Access Control



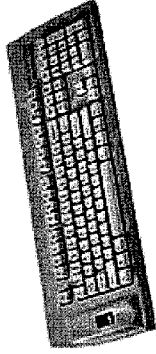
Cost of Securing a Computer with Biometrics



Integration into PC Infrastructure

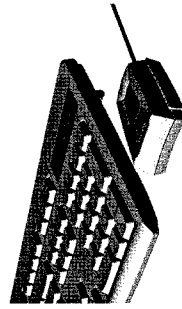


IDT DFR200 OEM module



Keyboard

- Fingerprint Identification Reader built into existing PC peripheral devices



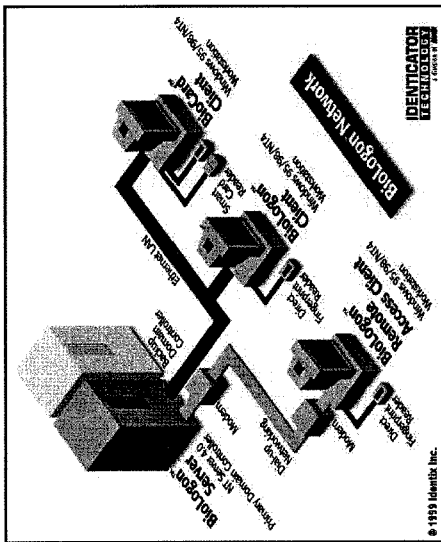
Standalone



identix

BioLogon™

- MS Windows 2000/98/95/NT 4.0
- Workstation, PDC, BDC
- Integrated into MS SAM
- Support Various Integrated Peripherals
- Enrollment Wizard
- Variable Thresholds
- Multiple Finger Enrollment



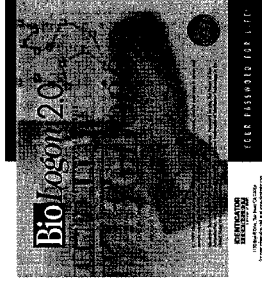
BioLogon™

- Client/Server Software
 - User / Administrator Friendly
 - Simplifies Logon Process
 - Decreases Cost of Network Ownership
 - Seamless Integration
 - Client/Server 3-5 MB
 - Biometric template size 256 bytes

BioLogon 2.0



BioLogon Client



BioLogon Server

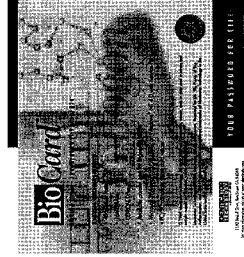
identix

BioLogon™

- Security Pack
 - BioSafe
 - Encrypt/Decrypt files on Desktop using Standard RSA encryption algorithms
 - BioShield
 - Locks Applications
- BioCard Client
 - Enables Token Layer (Smart Card)



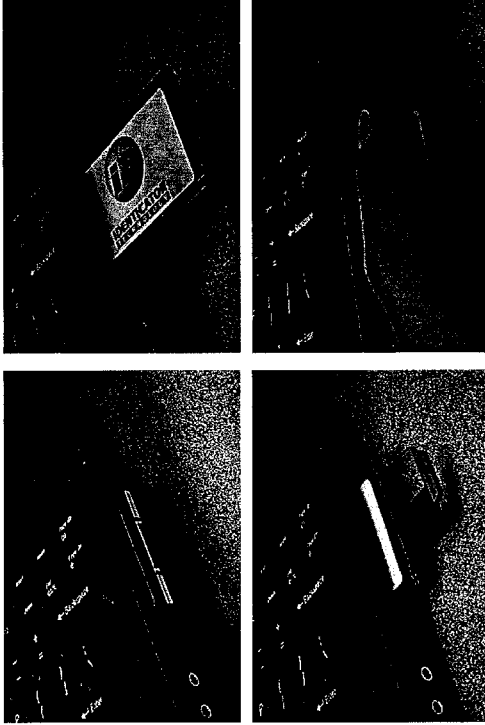
BioLogon Security Pack



BioCard Client

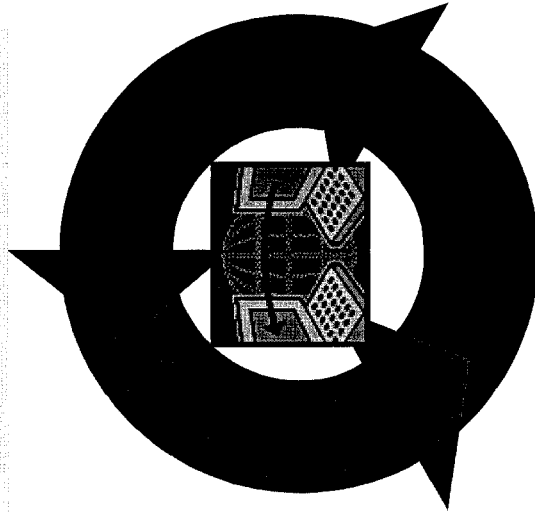
Mobile Solutions

© 2008 Identix Corporation. All rights reserved. Identix, the Identix logo, and the Identix logo are trademarks of Identix Corporation. All other trademarks are the property of their respective owners.



Standards Activities

- BioAPI Consortium
- NIST Common Biometric Exchange File Format
- ANSI / NIST Standard for Fingerprint Data Interchange
- International Biometrics Industry Association
- Association Motor Vehicle Administrators (AMVA)
- Banking Information Technology Secretariat
- NSA/GSA X.509 Standard



Biometric Industry Efforts

Biometric Consortium
www.biometrics.org

International Biometrics Industry Association
www.ibia.org

BioAPI Standards Organization
www.bioapi.org

identix

For More Information

M. Paul Collier
Identicator Solutions
12300 Twinbrook Parkway
Rockville, MD 20852
Phone: +301-468-2444
Fax: +301-468-6455
E-mail: pcollier@identicator.net

Web Site: <http://www.identix.com>

identix

IDENTIFICATOR
SOLUTIONS
a division of *ANADAC, Inc.*

Mr. HORN. Let me just ask you about the biometric technology chart. While going over to vote and coming back, I talked with Mr. Tauzin, who is very interested in this, and he is going to have a meeting of the Internet group here on May 19th and 20th. So we hope what will come out of this testimony of yours and the previous panel a couple of weeks ago will be helpful.

One of these patterns is rather interesting to me. A few years ago, the Immigration and Naturalization Service put on a demonstration in a room in the Capitol, various things they could do to identify people. I was fascinated by the one where you put your hand in.

Is that on your chart, the vein patterns, paren, hand? Is that the one, or is that separate from that?

Mr. COLLIER. They are different technologies, though they are essentially similar.

Mr. HORN. Looking at the spread of your fingers, and they claimed it was better than fingerprints.

Mr. COLLIER. Well, we all have claims, I guess. The hand geometry system used by the Immigration and Naturalization Service, I think, were deployed in their INS-Pass Program and are still working to this day. Hand geometry is a viable technology. Fingerprints appear to be what the government has embraced because of the long experience with them.

Mr. HORN. Yes. So is there any sort of works on this that will give us an idea as to which is the better of the two between fingerprints and the hand pattern? Anybody research that?

Mr. COLLIER. I believe they both have their place. There are about 15 different biometric disciplines. There is no one discipline that fits all scenarios. The real issue comes down to cost per seat, per deployment. Some of the biometrics available are extremely effective, but may cost \$100,000 per unit to deploy. It is never going to see widespread deployment at that cost.

There are studies that have been done by the National Security Agency that are available. There are studies done by the National Biometric Test Center at San Jose State University, and Sandia Laboratories did some studies several years ago for the Department of Energy.

Mr. HORN. This is a question really for all of you, and that's based on the testimony. It appears many computer security tools are free or at little cost, and I guess the question is this: Why aren't more agencies taking advantage of all the security tools readily available to them? What is your experience on that?

Mr. BROCK. Well, I think that many tools are free, are readily available. Many of the tools you can actually download from the Internet or are made available from vendors free or low charge.

What we have seen is that agencies inconsistently use the tools, or they don't provide the appropriate training to understand how to use the tools, or they don't even know how to turn the tools on. So while the tools are available, they are just not used properly. That seems to be the biggest problem that we have found.

Mr. NELSON. I would agree and would add there is motivation and resources involved. As I said in my testimony, nothing is free because there is a labor cost. Many system administrators were sort of pressed into the job. They weren't well-trained. It is a new

field, and many of them are overloaded because management doesn't appreciate the importance of security, so that even if they know in principle the tools are available, finding the time to acquire them, to understand them, and to deploy them and to then take action based on them is a pretty big load.

As I indicated in my testimony, at NASA we have deployed uniform suites of commercially acquired tools because our study—I won't say it was a thorough study, but we looked at the cost of labor and the ease of use, and we found that the commercial tools were a better buy for us, but then augmented by selected free tools. No tool is perfect.

Mr. HORN. I was interested in your testimony where you put the stress on training and supervision, and you remind me now on management we put a measure through here, and it is, I think, almost law, or it is still in the Senate, and that would be to give the new President, whoever that is, a chance to relate to the top management that he would bring in. Ordinarily, between the Cabinet, the independent agencies, that's about 30. Then you have got about 300 Commissioners and Under Secretaries, so forth.

I think we definitely ought to get on that agenda, then, their understanding of this type of security management. If it goes up that high, and they don't understand it, I think it will—and staff will note this, and we will put it in maybe even as two words or something in what is coming out of the Senate.

Mr. NELSON. What we did at NASA at the Administrator's direction, the Chief Information Officer and I—I am Deputy Chief Information Officer—visited each of our 10 centers and headquarters and gave hands-on training briefings to the center senior and middle managers.

Now, that wasn't a lot of time, but it emphasized that we meant business, and we talked about metrics. We talked about actions we were taking. We talked about their responsibilities. It seems to be working. So I would commend the administration to think of something like that.

Mr. HORN. Yes, I agree. The way we got leadership finally on the Y2K thing in the executive branch was when Mr. Koskinen was picked and went around and sat down with all the Deputy Secretaries of each department to get them to understand that this was serious business.

Any other comments on that? Mr. Collier.

Mr. COLLIER. The tools that are available at little or no cost need only the person's desire to implement them. We constantly see Windows basic tools for securing systems totally inactive. It is a tradeoff between security and convenience. Biometrics, we feel, brings both to the party in the sense that it does give you the speed. It is not something else to flip on and flip off. It is not something else lengthy to remember. If we look at what we have done at passwords to overcome this ability for people to break into our systems by finding out what our passwords are, it is not the dog's name anymore; it is not a simple thing that you can keep for a year, or your wife's maiden name. It is an upper/lower case, full eight-character ASCII 2 set. It is extremely difficult for anyone to remember that. Change it every 30 to 60 days, and give them three or four to remember, it can bring about a problem.

So I think the real issue is utilizing the tools that are available and making the operators understand that the security is important at the risk of what little inconvenience it is going to cause.

Mr. HORN. Well, with reference to this subject, where on the Internet can organizations and citizens find these tools? Is it there?

Mr. NELSON. Let me speak to that. In my testimony I indicated two sites. One, is our own NASIRC site, www.nasirc.gov. The second, that I indicated was the Carnegie Mellon CERT that I think Jack also mentioned. They have a good set of tools.

With search engines and other news groups, it is probably a half-hour to get started. I mean, this is very easy to do. This is probably the easiest step. There is the step of, well, what is good and what is not so good; what is easy to use, what is not so good—what is not so easy to use. But access is the easy part.

Mr. BROCK. I would agree with that.

Mr. HORN. Intrusion detection tools can either be manual or labor-intensive. Is there a better way to monitor potential intruders?

Mr. BROCK. Intrusion detection tools are a necessity. What is difficult about intrusion detection tools is actually following up. I mean, if you—you have an intrusion detection tool, and you are logging in intrusions, you need to followup. The issue that we found at many agencies is if they have intrusion detection tools, and they are logging them in, frequently they are not following up on the incidents to take corrective action or to do something to stop the intruder. That's why they are labor-intensive. You have to look at each one individually.

I can't recall any intruder detection tool that would automatically fix the problem or stop the intrusion. At some point somebody has to intervene.

Mr. NELSON. Let me speak to that. Right now, and I agree with what Mr. Brock said, right now it is manual, it is labor-intensive. At NASA we require that every incident be reported to the IT security manager at the center, and then to our NASIRC, which we use as a coordination means.

So we send out encrypted alerts to our security people at all centers based on the incidents reported by each center. Many of those incidents are detected by the intrusion detection tools. The securities managers followup with the system administrators to get things fixed. Again, that's quite manual.

What we are looking at and what I would encourage the industry to work harder on is automated, if you will, artificial intelligence means to identify intrusions and identify a recommended course of action. One of the things we are looking at doing, we have not done it yet, is to gather from each center—see, we are using the same tool—into a centralized analysis location what those tools are reporting and apply the artificial intelligence to the set of reports. We find that if one NASA is—one NASA center is being attacked, often several others are. These are coordinated attacks. But I repeat, the artificial intelligence tools for analysis do not appear to exist yet. It is an area that NASA is tracking carefully, and we hope that in the next year or two we will see something we can start to deploy.

Mr. BROCK. If I could just add to that, Mr. Chairman, that's true. The intrusion detection tools are very immature at this point, and

they are evolving. Again, another risk is that as—is once an agency or an individual buys a tool, that tool is changing rapidly, and the intrusion detection tools, they are changing very rapidly, and they are not at a stage of maturity now where they are going to provide the final answer.

Mr. HORN. Is there any way you can tell with the intrusion that the—the type of computer is doing that, or is it just hopeless? Because I am looking at individuals have one capacity generally; foreign governments do have another capacity. If any of them have something such as a Cray computer in terms of what they can spin around and test things against to break through particular firewalls, I am just curious about that.

Mr. NELSON. Usually we can tell what is called the source Internet protocol address, and that identifies the location of the attacker fairly well. Occasionally those addresses can be what they call spoofed, which means they are faked, but typically we can identify that.

Now, your discussion about the difference between an individual and a foreign country, I wouldn't make too much of that because groups of individuals are acting together, and the power of modern, even personal computers and certainly work stations is fully adequate to mount an attack that is very serious.

So we pay a lot of attention to individuals. Obviously when we sense that it is a better organized group, all the way up to a government, we pay particular attention to it, but we wouldn't want to make too fine a point on that distinction.

Mr. HORN. Any other thoughts on that?

OK. Mr. Brock, you mentioned in your statement that poor security planning and management is, "the rule rather than the exception." So why is this posture the rule and not an exception?

Mr. BROCK. I wish there was a real simple answer to that and that it would be easy to fix. It is, unfortunately, like a lot of other issues, and very similar to the Y2K issue, is that it—the actual computer security break-ins, the failings there are technical. The correction is a management issue. There have to be resources devoted to it. There have to be dollars, and there has to be training, and the people that own the processes, that own the information, that are accountable for that need to be accountable for computer security. That is not the case, and until that ownership occurs, I don't think you will see widespread, systematic repair of the poor computer security problems.

I think that happened in Y2K, in large part because of the intensive oversight in Congress, in large part because of Mr. Koskinen coming on board, in large part because Federal managers were made aware there was a crisis. Those three elements have not yet been put in place for computer security.

Mr. HORN. Well, you have put them very well, and that's what I was leading to, in the sense that when Mr. Koskinen came on board as assistant to the President, he worked with the Chief Information Officer's Council and got the best out of them. And I guess I would ask, does the Federal Government need one organization or one high-ranking information technology officer to coordinate security planning and management? Do we need to continue a sort of Koskinen situation and relate it to security?

Mr. BROCK. That's an excellent question. I guess when you start off saying that's an excellent question, that means you are going to be wondering about my answer.

Mr. HORN. Is there an excellent answer?

Mr. BROCK. I hope so.

Mr. HORN. We are college professors. We ask questions. We don't answer them.

Mr. BROCK. Well, I will go ahead with the answer now.

The—I believe there needs to be a Federal CIO. I think very strongly that the information management issues, the information technology issues that run across agencies are serious. It is not just in computer security, but it is in terms of how you control your investment dollar. It is do you have an architecture that will support your business needs and your technical needs. There are a series of issues that need to be addressed on a consistent basis.

I think the CIO Council has done a reasonable job of looking at some of these, but they are not in power. They don't have budget. They don't have staff. They are volunteers on this. There needs to be someone who is providing more direction, more leadership.

Now, in terms of—and I believe that in this case a Federal CIO would also be responsible for computer security.

Similarly, if you decided that computer security was an important issue in terms of critical infrastructure protection, where you were also involving the private sector and you were involving physical security as well, I could easily see a role for a national coordinator for critical infrastructure protection that might be separate from a Federal CIO who would be dealing primarily with agency responsibilities.

Mr. HORN. I have one reservation here, having been in the largest educational system in the country, which is California State University system. When you put somebody in the system headquarters, everybody sort of says, oh, that's their problem, and pretty soon they forget that it is their problem. They are the campus administrators; that's where it happens. It doesn't happen in headquarters. They never educated a student in their life. A university does, and so do our departments. They are mission-oriented, and they are producing things. I worry if, say—to say, well, that isn't my business, let those people over in OMB; or if we can separate it into the Office of Management or the Office of Budget, and that's what worries me. Doesn't that really sort of let up the heat on the individual, the independent agencies, Cabinet departments?

Mr. BROCK. If I could go back to the Y2K experience, I think that even though there was a national coordinator with Mr. Koskinen, he clearly held agencies accountable for their actions, as did the President. I was here for several hearings, and you were holding those agencies accountable.

I think you can keep the heat on the agencies. That's where the responsibility lies for good computer security.

Mr. HORN. Right.

Mr. BROCK. But the focal point, the Federal CIO, could assist in that. I do not think that the Federal focal point should become the stopgap; that this will solve the problems. That still has to occur at the agencies, but certainly a CIO at the national level could propagate good practices, could leverage resources that were avail-

able to that individual and serve a role, frankly, very similar to the one that Mr. Koskinen served.

Mr. HORN. Yes. We had a specific time period that wasn't going to be for 10, 20, or 100 years. It was just going to be a few months, and that's really what it boiled down to. And the job was very well done obviously, but that's—I need that balance, I think.

Mr. BROCK. Yes.

Mr. HORN. So you don't have people say, hey, it isn't my problem, they do that over there, and wash their hands of it. I don't think that will help us at all.

Mr. BROCK. No, it would not.

Mr. HORN. Yes. But we certainly ought to have somebody that had the right skills, people skills, so they aren't some czar. The czar makes my spine shudder. But so that they are a coordinator in getting people in the various systems that overlap to work together, that's the way I would view that coordinator role.

Mr. BROCK. I would agree. I think that the success of any coordinator or official like that does depend very much on that individual's personal skills in terms of working with a very diverse group of organizations who have different needs and different objectives. That's a difficult job, very hard job.

Mr. HORN. That's right.

Mr. Nelson, any thoughts on that?

Mr. NELSON. Yes. Just to add a bit to Mr. Brock, I agree up to possibly whether a CIO, Federal CIO, is warranted. As you know, that's being debated within the administration, and I won't take a position on that.

I agree with him that one does not want to separate the computer security aspects from other aspects of management. We are focusing on computer security today because, indeed, it is a new problem. I am an optimist, and I think we are going to get this problem under control, and if we have a legacy of a fragmented management approach, it is going to take on a life of its own.

A number of years ago, I worked on environmental protection and on OSHA problems, and one of the things that I pushed on was to reintegrate those functions. I called them the OSHA Mafia, back with management, because management was abdicating its responsibility, and, frankly, the Mafia in some cases were running rampant with things that didn't make sense. Now, that's a very personal observation. It's not NASA's observation. But my experience in this area tells me that you want to integrate, you want to set high standards, you want to measure, you want to train, but you put the responsibility on the people who have to make the tradeoffs and get the job done.

Mr. HORN. I agree with you completely on that. You say it very well.

Mr. Collier, any further thoughts on this?

Mr. COLLIER. Mr. Brock and Mr. Nelson both mentioned that communication between different agencies and even within a particular agency is a critical element here. Within the government, of course, the Critical Information Assurance Office paper that came out this past year points to that. The CIOs do have several venues in which they talk to each other. The Government Informa-

tion Technology Services Board, I think, has done a good job in at least keeping the communication flowing between agencies.

But I would tend to agree with you that to establish an individual to take on this responsibility may not be the proper way. The proper way to do this would be probably to continue the communications, the lines of discussions, between agencies.

Mr. HORN. In your statement, Mr. Brock, you mentioned that your audits have shown that Governmentwide computer security is generally weak because current policies and controls are not operating effectively. You also stated that the General Accounting Office audits frequently find the same vulnerabilities over and over and over again.

In your opinion, what would you specifically suggest that agencies do to strengthen existing policy or to create stronger policies? What is your thinking on that?

Mr. BROCK. The—you are correct. Our reports have found the same problem over and over again.

A couple of observations. First of all, many of the policies have no relationship or a limited relationship to the problems that we are finding. They are not specific to the issues and problems that are within an agency. We believe that policies and procedures need to be based on the risk that the agencies are facing, and if you do a good risk assessment, you can then, in fact, determine policies and procedures that will minimize or mitigate those risks.

Second, most agencies aren't testing their controls. They rely on GAO or IG to come in and do the test, so there is too limited information within the agency, one, about what the risks are and whether the policies would be reflective of reducing that risk, and second, are the controls in place working, are they being tested? Those are the things that we would do to, one, develop policies that are appropriate, and, second, to strengthen existing policies to make them more responsive.

Mr. HORN. You also suggested that agencies develop and distribute lists of vulnerabilities. To whom would these lists be distributed?

Mr. BROCK. Well, first of all—

Mr. HORN. Should it be GAO; should it be OMB; what, CIO Council?

Mr. BROCK. Everyone.

Mr. HORN. All of the above?

Mr. BROCK. First of all, let's start within the agency. I believe I mentioned earlier within some agencies we would go to, they do not distribute such lists within the agency so that people that are literally down the hall are not getting these lists. So, first of all, you need to start within the agency.

Second, there are other organizations, such as the CERT-CC, the Carnegie Mellon, the Fed CERT, the GSA runs, organizations that do have distribution mechanisms that are appropriate as well.

Mr. HORN. Yet Dilbert and the cubicle is broken down?

Mr. BROCK. Yes.

Mr. HORN. Mr. Brock, you stated that establishing a framework for managing security is important. What specific elements of the framework are missing at most agencies?

Mr. BROCK. If I could indulge Mr. Gilmore to put up the circular chart, the wheel.

The risk management cycle, we believe, is the framework. I will go back to an answer I just gave you, that the framework has to start with a central focal point, the accountability. From there, determine what the risks are, develop controls based on that risk, promote awareness, and then continuously monitor and evaluate. That's the framework.

Certainly there are things that you can do independent of that framework, or you don't have to implement everything in that exact cycle, but it is dynamic. It is continuous. The threat is growing. The threat changes. The technology grows. The technology changes. The services that an agency provides change. So the risk management cycle has to roll on a continuous basis.

Mr. HORN. So it is interactive in many ways?

Mr. BROCK. Yes, sir.

Mr. HORN. Gentleman, Mr. Nelson, Mr. Collier, what do you think about that approach there, just as one vision?

Mr. NELSON. Yes. I agree with Mr. Brock. I would like to give you some examples of what we are doing at NASA along these lines.

I said before that it starts with management. We have identified what we call special management attention systems. These are important computer systems for NASA's missions, and we are requiring 100 percent completion of security plans for those systems by this year, and we have asked our Inspector General to audit that, including the involvement of management in those plans and management signature on the readiness of those systems to operate.

But we have had to operate in parallel because the risk is too great. So at the same time we have identified what we call the top 50 vulnerabilities in NASA, and we have distributed that list to every center. It was done by consensus, not somebody in a closet, but using the tools that I described, all of our systems are being audited for the presence of those vulnerabilities. When those vulnerabilities are detected, management is informed of them and asked to correct them, and then those systems are rescanned.

Now, management, if in its interest it believes that some of those vulnerabilities must maintain because the risk is tolerable and the loss to mission is too great, they can do a waiver. But this forces them to act even before some of their plans are completed, because we think that it is too much of a crisis.

Mr. HORN. OK. Any other comments on that question?

Mr. COLLIER. I would agree that it is a management and policy issue. When the Department of Defense began its studies of biometrics back in the late 1980's, early 1990's, there was as much emphasis placed on the people interface to biometrics as there was on the technology side.

I found that a very refreshing model. I mean, the human element is really what is the issue here. Technology pretty much does what we make it to do, and it keeps on doing it. In the area of security, however, the Department of Defense studies, especially of the National Security Agency, involved the study of time, motion, and the people's acceptance of a new way of doing things, and labor was definitely a part of the decisionmaking process.

I think that's a critical element in moving forward, to remain dynamic enough to meet the threats as they continue to improve on a day-to-day basis.

Mr. HORN. Mr. Nelson, any further comment on that question?

Mr. NELSON. No, thank you.

Mr. HORN. Mr. Turner has joined us. I am delighted to yield such time as he may need for questioning.

Mr. Turner.

Mr. TURNER. Mr. Nelson, I wanted to ask you if you could describe for us the kind of computer intrusions and attacks that you have experienced. We talk about this all the time, and I don't really have a good grasp on the scope of the problem. So can you quantify that and maybe give us some specific examples of how some hacker has invaded your system, what the consequences have been?

Mr. NELSON. Yes.

Mr. TURNER. I know that we always read this is a widespread problem.

Mr. NELSON. Yes.

Mr. TURNER. I don't think we have a real feel for how widespread it really is.

Mr. NELSON. First of all, NASA experiences a lot of attacks, hundreds to thousands per month.

Mr. TURNER. You say hundreds to thousands?

Mr. NELSON. Hundreds to thousands—of serious—to thousands per month of serious attacks.

Mr. TURNER. Hundreds to thousands?

Mr. NELSON. Yes. And we are not unusual, although we may be are slightly favored.

Let me give an example of an attack which has several of the elements we have been talking about in our testimony.

I am not going to describe the center, but in this particular instance a system administrator observed that someone from a foreign country had logged into the computer and had no reason to think why that person should have—should be able to log into the computer. He did this by examining records logs, so he was doing the right thing.

Now, he found by looking at the log that the person had used a well-known vulnerability to take over that computer; in other words, to achieve what is called root access. That's like god of the computer. You can do anything with the computer if you are root.

Then the person used that vulnerability and his godlike powers to install what is called a password sniffer. This is software that observes the network traffic flowing by and looks for packets that have passwords in them. And he was able, the intruder, to grab a number of passwords, some of which were for accounts at another center. So using those passwords and then the ability to log on as a user, the attacker went to another center and attacked several other computers.

Now, the sad part about this was that the initial vulnerability should have been fixed. The system administrator thought he had fixed it. He installed what is called a patch. It is a thing like a Band-Aid; it is like a patch that changes a software to get rid of the vulnerability, but the patch didn't take. It was a defective in-

stallation process, and the system administrator didn't know it. So he was hit twice with the same vulnerability.

Now, we have had other attacks, and we keep track of how much they cost, that have had a direct cleanup cost in time and resources approaching half a million dollars, one attack. Of course, it affected a lot of computers.

Mr. TURNER. You say one attack cost half a million dollars?

Mr. NELSON. Approached half a million, a little under. The numbers are not, of course, audit quality, but these are expensive attacks. It took—in the case that I am referring to of almost half a million dollars, it took about a month to put all of these computers back together again. It was a major problem.

We have had centers actually take themselves off the Internet, in other words totally sever connections with the outside for a brief period of time, because they felt that they were being attacked, the risk was too high, they needed that time to fix things up.

Now, the incidents that I am describing now are a year or two old, and we don't have such bad problems now, but we still get significant attacks.

Does this help? Does this give you a sense of—oh, one area that I didn't describe is theft of data. We had an incident not too long ago where substantial number of documents were stolen by an Internet attack.

Mr. TURNER. And what—were those sensitive documents?

Mr. NELSON. No, fortunately not. They were copyrighted. They had commercial value. They were not sensitive. And these particular documents were not resident on a NASA computer. It was a NASA account that was used, and there was a serious weakness in the vendor's security. But that's an example of an attack that NASA was peripherally involved with.

Mr. TURNER. So you say there are hundreds to even maybe 1,000 attacks per month?

Mr. NELSON. Correct.

Mr. TURNER. Now, have you been able to successfully determine the source of any of these attacks? Or do these things just go on daily, and you try to prevent them, but you don't know who did it?

Mr. NELSON. We can determine the source of most of them, at least within the country, and maybe the organization. And we work closely with our Inspector General and then with the FBI, and several of these have been prosecuted and the perpetrator convicted. In a—on a regular basis, if we see an attack, we inform the organization that the attack is coming from, and often the attack is from someone not connected with that organization, but someone who has seized a computer, seized meaning this root access, god powers within the organization. The organization may not know it. That could be a government organization or a private organization in this country or abroad.

So one wants to be careful saying we are being attacked from a certain country; they must be hostile. Maybe they are the victim.

Mr. TURNER. So there have been some convictions that have resulted from your investigation?

Mr. NELSON. Yes, sir. Yes, sir.

Mr. TURNER. Would it be fair to say that the vast majority of the attacks, that the source of them are—that you never quite figure out who did it?

Mr. NELSON. Yes.

Mr. TURNER. Or where they are from?

Mr. NELSON. Yes. Not in who the individual was or what their motives were, that's correct. And attack isn't necessarily successful. I want to make it clear that when I talk about hundreds to thousands of attacks, I am including all of the incidents that we gather metrics on. The successful attacks would be a lot smaller, and increasingly we ward off those attacks. We use another metric of what is the success rate of incidents, and we are seeing the numbers turn over. It is sort of a nice payoff for the hard work we have gone through in the last couple of years that our numbers are getting better. The attack rates are going up. The successful attack rates are going down.

Mr. TURNER. Tell me the examples of intrusions from foreign governments or agencies of foreign governments.

Mr. NELSON. I don't have data on that that I would be confident in saying, even in a conversation. So I am sorry, I do not have any data on attacks by foreign governments that I would have any confidence in reporting.

You know, it is hard to know, when you have an attack from an IP address, even if that is located within an agency of a foreign government, is that the activity of a foreign government. To the best of my knowledge, we have no evidence of NASA attacks by agents of foreign governments, but I do not have high confidence in that statement because we do not have good data.

Mr. TURNER. The convictions that have resulted from the efforts, what kind of individuals are we talking about that have actually been convicted of a crime?

Mr. NELSON. Our Inspector General would be a lot more authoritative on this, but I believe they have tended to be fairly young males working either alone or with others of like mind, but at least my knowledge is that they do not appear to be part of what one might call organized either crime or terrorism in the conventional sense. Their prime aim, as I recall—but I think if you would like we could submit for the record a response from our Inspector General, I could request it—but as I recall, they have not been industrial espionage cases or the like.

Mr. TURNER. I do think it would be helpful, with the chairman's permission, to ask you to at least give us some indication maybe for the last 2 or 3 years of the number of attacks, how they have been resolved, and whatever information you can provide us about the source of them, because at least by looking at it as a whole, we would get some picture for us to look at of how serious this problem really is.

Is that possible to put that kind of data together to give us an overview?

Mr. NELSON. Indeed, it would. If you will give us just a little leeway.

We try to not advertise the successful attacks. Our experience is that one of the motivations for attackers is the recognition, if you will, the thrill. We are very leery of playing to that.

Mr. TURNER. I suspect that your reticence on that point is shared by many people in various agencies of the government, and I think one of the difficulties that we have as a committee in trying to address this problem is trying to get some data together to indicate how serious this problem really is.

Mr. NELSON. We would be eager to work with you on getting data that is helpful to you.

Mr. TURNER. When you deal with these kind of intrusions, do you rely upon NASA employees, or do you rely on contractors to help you resolve them?

Mr. NELSON. Both. Many of NASA's services are now operated by contractors, and so we have integrated those contractors into our operations. In our testimony—in my testimony, I mentioned that we have a draft regulation out for comment that would require the same training standards for our contractors as for ourselves. NASA has not outsourced or not contracted out our security responsibilities. So where we have contractors operating systems within our centers, or otherwise directly attached to NASA, we retain the responsibility and the capability for detecting and responding to attacks.

Now, that response may be asking the contractor to do something. Since they are well-integrated now into our planning, they are eager to do that.

I think the system is working fairly well, but it has added a complication of crossing these contract boundaries.

Mr. TURNER. Is it possible for an intruder to compromise the success of any of our missions? I know you have had a tremendous problem recently with success in some of the Mars missions. Is it possible that a problem could be created of that nature by an intruder into our computer systems?

Mr. NELSON. We take pretty strong security precautions for mission-critical systems. Having said that, there is always a possibility. We are into risk management. Risk avoidance is very difficult. We do, though, take, as I said, very strong precautions, including in some cases simply severing the critical system, planned severing from any outside communication to minimize that risk, but we are talking about risk management, not risk avoidance.

Mr. TURNER. Thank you, Mr. Chairman.

Mr. HORN. Well, we thank you. That was a very useful interchange, questions and answers.

Let me go back, Mr. Nelson. Has your top 50 list of vulnerabilities been distributed outside of NASA?

Mr. NELSON. Not to my knowledge. It was a list that we arrived at working among ourselves, and it is a list that we have programmed into our auditing tools. So it is, in effect, automated now. But I am not aware that we have distributed it outside the agency. There are other agencies that are doing similar lists, and I think the overlap would be pretty large.

Mr. HORN. Well, would it be helpful if in a report from this subcommittee that we use some of that information if there are ones beyond NASA that differ, and then the question would be does that encourage hacking or doesn't it? But how we deal with it, I think we have to get the word out.

Mr. NELSON. We wouldn't want it known what number 51 is, and 50 was a good round number, and that 50 will change. It is partly getting well. We have had to beat on this one, as I indicated earlier, to get managements attention, but we expect that next year's top 50 will be a different list, and it may not even be 50. But, yes, with appropriate precautions we would be willing to share that list, certainly, with responsible people in other agencies.

Mr. HORN. On Mr. Turner's point, I just suggested to Mr. Ryan that we find from Justice how many have been jailed and where are they. I know a few are in the Atlanta prison, but I think it is good to get at least some of them. We don't have to make heroes out of them. We can say Mr. Blank and Ms. Blank or whatever, because I don't want to have this be the award system for hackers.

Let me ask you, again, Mr. Nelson, another thing. You gave a very interesting chart when you said you are spending roughly 2 percent of the funding for information technology on security provided adequate protection. Two percent seems like a very modest amount to spend on security, so I guess do you think that's pretty low, and should we invest more?

Mr. NELSON. I can only speak for NASA, and we do gather budget data on our actual costs. Our information technology budget as a whole is about \$2.1 billion, and our fiscal year 2000 expenditure on information technology security is about \$46 million, which is a little bit over 2 percent.

Now, we don't know that that is optimally allocated. So I would say at first, my initial reaction is that NASA—and that increased quite a bit, by the way, from 1999 to 2000. But NASA is now spending about the right amount, and it is a case of efficient allocation so that we hit the most important things.

Mr. HORN. So you think you are at the right level of spending on this then?

Mr. NELSON. Approximately.

Mr. HORN. OK.

Mr. NELSON. Yes. Now, Mr. Collier, in your written statement, you explained that the prevalence of computer passwords written on the back of computer mouse pads, on desk leaves, and even on paper attached to computer monitors do exist. I know what you mean. I think it is all around Capitol Hill, too.

In addition, you stated that remembering a PIN, the personal identification number, is a key piece of computer security. In your opinion, what can individuals do to better recall passwords?

Mr. COLLIER. Aside from memory exercises, if we are going into this 8 character password with, again, a full keyboard set of characters, I think the idea is to do something to move away from these complex passwords. The positive user authentication model that I presented earlier is an effort to do just that. Again, we have the human being factor here at the edge of the envelope.

Our company has clients, for instance, in the wire transfer business where they have 25 passwords to remember. Now, unless you are the Great Kreskin, it is pretty difficult to do that. So I think rather than trying to formulate ways to help people remember passwords, we have to find ways to eliminate them entirely, and I think the positive user identification model, which I think the

DOD originally had come up with 10 years ago, is a move toward that.

Mr. HORN. Does that mean a certain unit has to be built on every machine to do that in terms of the fingerprint and all of the rest?

Mr. COLLIER. Biometrics are certainly one of the legs of the stool. The cost, again, is coming down greatly. Right now we are seeing it move into the mainstream, certainly in the commercial world, protecting enterprise systems within large corporations. The Federal Government is doing it at the division and command level now, and I think it is just a matter of time before we see biometrics not only in computers, of course, but in many, many areas of our lives where we have to remember passwords, PINs, and the like.

Mr. HORN. If you had the, say, thumb identification to access your particular personal computer, is there any way a hacker getting into that would be able to digitize the lines and everything else so they could duplicate that?

Mr. COLLIER. At the direction of the computer industry and the Department of Defense, primary responsibility from the NSA side of things, we have addressed the issue of intruder attacks, we do encrypt the signals coming out of the scanner, so they can't be sniffed. Our product in the sense of the templates is part of the operating system which is part of the layered security shell around the password protection. We do secure sessions between all pieces of hardware, as well as between client and work station. There have been a lot of efforts put into making this stuff spoof-resistant. James Bond might still be able to get in, but not the average user, that's for sure.

Mr. HORN. Well, I was interested when one of you compared the need for looking at how you divide the issues in computer security are very much like a responsible accounting operation when you are handling a lot of money, and you want more than one, and my chief auditor said many years ago—he said, make sure everybody takes a vacation. The system—when they found one in another system in California where the vice chancellor just happened to be buying bales of hay for his ranch, but not the university ranch, he was charging it to the university, and the only way they found that was when he finally took leave and somebody said, gee, this is strange, and that was solved.

That's, I think, what we have to do here. Is there something along that line that we ought to be telling everybody that runs a computer center in the Federal Government and how we could apply what people do in the finance and auditing in universities and corporations for standard practice?

Mr. Brock.

Mr. BROCK. Segregation of duties is perhaps one of the most absolute basic controls there is for any type of operation, whether it is financial matters, as you were talking about, or computer security.

In fact, when you look at any critical operation from beginning to end, you can make breaks in there where you say, we are going to have a division of labor, and in computer security, if you were looking at a process of changing software, you can make breaks from the people who make the change to the people who do the

testing to the people who do the installation, to make sure that there is an independence there.

You could do that for other aspects of security as well.

Mr. HORN. Well, in other words, in your opinion, are Federal agencies susceptible to having one individual either intentionally or inadvertently render the computer system useless due to the lack of segregation of duties or separation of duties involved?

Mr. BROCK. I don't have the exact numbers now, but we have—maybe I do have the exact numbers.

Mr. HORN. Ms. Boltz, glad you came today.

Mr. BROCK. We don't have numbers, but we did identify, for example, at the Department of Defense and VA that system program and security administration duties were combined. So the people who were establishing the controls were also doing the programming.

At the FMS, we were saying that programmers had access to production data. So, in both cases they were able to combine pieces of information; if they had chosen to, could have taken over programs and assumed other responsibilities as well.

This is fairly common. In some respects, it is done not out of a malicious intent. It is done because I think, as Mr. Nelson alluded to, you have too few people trying to do too many things.

Mr. HORN. Any other thoughts on that, Mr. Nelson, Mr. Collier?

Mr. NELSON. Yes, I would say I agree with Mr. Brock. However, in the scientific and technical area, the terminology may be different, and so one has to be a little careful not to be too rote in the prescriptions. What applies well to a financial system may not apply very well to a scientific data analysis system. The principles are correct, but the application has to be careful.

Mr. HORN. Yes. Mr. Collier.

Mr. COLLIER. You know, applications that we run into within the government, we have established some two-man rules in some cases. We have established complex procedures to ensure reduction in fraud, for instance, in transferring of funds, payment of benefits, etc. What I think biometrics and this security model bring to the party there, and that's what we are hearing from the government agencies, is we now have established the fact who was sitting behind the monitor when this fraud took place, not a matter of someone could have gotten my PIN or whatever. The banking industry has really embraced this because of the nonrepudiation issues and the home banking and wire transfers. As we get less and less on a face-to-face human basis, the problem increases, and they are trying to do something about the future that we know is going to explode before it does.

Mr. HORN. Thank you. Any other thoughts on that?

Mr. BROCK. No, sir.

Mr. HORN. One of my last questions here will be, in your opinion is the current legal framework, which includes the Computer Security Act of 1987 supporting Federal information security requirements, is that adequate? What needs to be updated or modified? Are there things that should be dealt with? Mr. Turner and I will be glad to move that legislation, if there is need for it. What does the CIO Council think on some of these things?

Mr. NELSON. Let me take that. In my opinion, the legal framework is pretty good. I am not a lawyer, so I will speak generally. But there is a potential problem that we are dealing with, and I think Mr. Brock alluded to it in his oral remarks. It has to do with classification.

The laws governing classification in this country are rather strict with regard to national security systems, and as the importance of information security has increased and the role of commercial and private systems has increased in their aid to national defense, then the question of where strictly national security stops and broader areas that are related to security starts. And so the particular problem that we are having is that we believe that within NASA a compendia, that is, lists, of open serious vulnerabilities, such as, for example, would be turned up by what we call a penetration test where we hire somebody or on our own to go through all of our systems and look to see how hackers would get in, that those lists are very sensitive, and my understanding—and we have been working with our legal staff and with the National Archives and Records Administration, which has ultimate classification authority, on the criteria under which these can be classified.

The issue is a little murky, but right now it looks like maybe they cannot be, not even at a confidential level. So it could be that some clarification of the extent of national security provisions in this gray area of civil systems closely allied with national security systems would be helpful.

Mr. HORN. Well, that's very interesting because this is the subcommittee that has oversight for the National Archives and the Freedom of Information, and we try to balance all of that. If there isn't a need for classification, it shouldn't be classified. So I would welcome any thoughts you have on that, and I know Mr. Turner would also.

So—

Mr. BROCK. Mr. Horn.

Mr. HORN. Mr. Brock.

Mr. BROCK. Can I have a moment of disagreement? I have been agreeing with Mr. Nelson all along.

I do not think the overarching framework is adequate. As we mentioned in the testimony, the Computer Security Act is based, I think, on an old way of doing things. It is based on an environment that existed before the Internet. It was based on a mainframe environment, and I believe that it was based on an environment where locks and keys were the prevalent security devices. It's system-based. It is not management-oriented. It misplaces responsibility and accountability. I think it needs to be overhauled.

I think there needs to be more emphasis placed on management accountability. I think there needs to be more emphasis placed on risk assessments and risk determination. I believe there needs to be more emphasis placed on independent audit and management audit so that controls can be evaluated. Those are not present in the Computer Security Act.

Now, as you know, there is no law against good management. There is no law or anything to prevent an agency from doing all of those good practices, but at the same time there is no law or legislation or regulation that really encourages that type of action and

then provides a lever or an oversight mechanism to the administration or to the Congress for assuring that that framework is being met.

Mr. HORN. Well, thank you, because that was the answer I was going to lead with a question, and I am so used to Joe Wilmington following me around the country on Y2K that I always asked, and now I will ask you and anybody from GAO, to what degree have we not covered the questions that we should have covered. And you have just nailed one down, and I appreciate that.

Would GAO and the CIO Council, Chief Information Officer Council, put their thinking caps on, and we would welcome taking a look at that again. We need to update it. It has been over two decades right now—or a decade and a half, I guess.

So are there any other questions any of you think—and you, Mr. Brock, in particular—what else should we get on the record that we haven't put on?

Mr. BROCK. I think that my last response covered the one item, and we are continuing to work with your staff on a number of computer security issues as well, particularly as they might relate to e-commerce and other initiatives that are coming up. We are pleased to have the opportunity today to discuss these items with you.

Mr. HORN. Well, we are glad to do it. We certainly welcome the comments of these witnesses, as well as the ones from our first panel. They were a very excellent group. Thank you, Mr. Collier, for coming.

Mr. Nelson.

Mr. NELSON. Yes, I would just like to maybe amend what I said so perhaps Mr. Brock and I can agree. In addressing your question on legal framework, I was responding from the standpoint of NASA or an agency as to whether the current law gets in our way of doing good things. But for an agency that does not wish to practice good management, a legal encouragement might not be out of order.

Mr. HORN. Well, that's well said.

I would tell you that this chamber operates not by consensus, but like a university does, and maybe NASA, but if we have 218 votes, we can do almost anything. But obviously we also could lose 218 votes if we haven't thought it through very well. So I thank you all.

I want to thank the staff that worked on this hearing.

You have been excellent witnesses.

J. Russell George is in the doorway over there. Gosh, are you getting framed now over there or what? Staff director and chief counsel, and he works wonders. Matt Ryan to my left, your right, senior policy director, and who is a GAO alumnus, as are a number of our people; Bonnie Heald, director of communications, seated in the back there; Bryan Sisk, our clerk; Ryan McKee, the staff assistant; and for Mr. Turner's staff, Trey Henderson as counsel, and Jean

Gosa, the minority clerk. And our court reporter today is one, and that's Mindi Colchico, and we didn't have to wear you out and bring another one in, I take it. So thank you for coming again.

With that, we are adjourned.

[Whereupon, at 12 noon, the subcommittee was adjourned.]

