S. Hrg. 105–786

INFORMATION SECURITY

HEARING

BEFORE THE

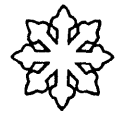
COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTH CONGRESS

SECOND SESSION

SEPTEMBER 23, 1998

Printed for the use of the Committee on Governmental Affairs



U.S. GOVERNMENT PRINTING OFFICE

51–643 cc WASHINGTON : 1998

For sale by the U.S. Government Printing Office
Superintendent of Documents, Congressional Sales Office, Washington, DC 20402
ISBN 0-16-057920-1

COMMITTEE ON GOVERNMENTAL AFFAIRS

FRED THOMPSON, Tennessee, *Chairman*

WILLIAM V. ROTH, JR., Delaware
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
SAM BROWNBACK, Kansas
PETE V. DOMENICI, New Mexico
THAD COCHRAN, Mississippi
DON NICKLES, Oklahoma
ARLEN SPECTER, Pennsylvania

JOHN GLENN, Ohio
CARL LEVIN, Michigan
JOSEPH I. LIEBERMAN, Connecticut
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia

HANNAH S. SISTARE, *Staff Director and Counsel*
ELLEN B. BROWN, *Counsel*
JOHN P. PEDE, *Professional Staff Member*
WILLIAM C. GREENWALT, *Professional Staff Member*
JOHN H. COBB, *Investigative Counsel*
MARGARET A. HICKEY, *Investigative Counsel*
LEONARD WEISS, *Minority Staff Director*
DEBORAH COHEN LEHRICH, *Minority Assistant Counsel*
LYNN L. BAKER, *Chief Clerk*

CONTENTS

WITNESSES

WEDNESDAY, SEPTEMBER 23, 1998

ALPHABETICAL LIST OF WITNESSES

APPENDIX

INFORMATION SECURITY

WEDNESDAY, SEPTEMBER 23, 1998

U.S. SENATE,
COMMITTEE ON GOVERNMENTAL AFFAIRS,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in room SD–342, Dirksen Senate Office Building, Hon. Fred Thompson, Chairman of the Committee, presiding.

Present: Senators Thompson, Collins, and Lieberman.

OPENING STATEMENT OF CHAIRMAN THOMPSON

Chairman THOMPSON. The Committee will come to order, please.

The Governmental Affairs Committee today is holding the third in a series of hearings on the security of Federal computer systems. Today's hearing will focus on the security of the private and sensitive information about each American that is kept on our government's computers. We will specifically look into the computer security problems at the Department of Veterans Affairs and the Social Security Administration.

Government computers must protect national security and the public's private and sensitive information from unauthorized disclosure. During our prior hearings, we focused on the fact that the use of information technologies as a tool of warfare and terror is becoming increasingly likely. No less important is the question of whether our government computers that hold the American people's sensitive and private information are secure.

The Social Security Administration computer system contains personal information on virtually every working American. If the Social Security Administration's computer system is compromised, the information about every single one of us in this room is available for the picking.

Equally, computer systems at the VA hold information that is vital to the health and welfare of our 25 million veterans. Sensitive information, such as veterans' medical records, home address, and benefit payments, must be protected. Knowing the medical history and home address of one of our Nation's military heroes is information that a dedicated enemy to the United States could exploit with substantial consequences.

But it is not just the heroes and celebrities that need to be protected. The Committee reports regarding identity theft and credit card fraud are examples of the fact that protections must be afforded to the average citizen. GAO has identified information security as one of the highest risk areas facing our government today.

GAO concludes that Federal agency computer systems are not being adequately protected, despite their sensitivity and criticality.

In the past 5 years, GAO has issued over 30 reports describing serious security weaknesses in major agency computer systems. The increased linkage of government computers, combined with poor security management, puts billions of dollars of Federal assets at risk of loss. In addition, vast amounts of sensitive data maintained by Federal agencies is at risk of unauthorized disclosure. Agencies' growing reliance on computer systems and electronic records has raised the specter that critical Federal operations are vulnerable to serious disruption.

Today, at the request of the Committee, the GAO will issue reports that raise serious concerns about risk to the public resulting from information security weaknesses. Gene Dodaro, Assistant Comptroller General, will testify on those reports and other findings of the GAO. The GAO cannot present their findings in their entirety because of the potential vulnerabilities they found, but has been able, with the cooperation of the agencies, to testify to many of the problems they uncovered at the VA and the Social Security Administration.

Using techniques widely available on the Internet, GAO tests show that the computer systems of both the VA and SSA are highly vulnerable. The VA operates the largest health care delivery system in the United States and guarantees loans on about 20 percent of the homes in our country. By gaining the level of access demonstrated by the GAO, sensitive information contained in the VA system, including financial data, personal information on veterans' medical records, and benefits payments, is vulnerable to being altered, improperly disclosed, or destroyed by outside hackers. The most disturbing fact is that GAO's penetration went undetected because the VA does not even have a monitoring system.

GAO also found that valuable personal information stored at the Social Security Administration is at risk. GAO's penetration of the SSA exposed vulnerabilities in the administration's computer system to both external and internal intrusions. These types of weaknesses place at risk the American people's most private information, their Social Security numbers, earnings, disabilities, and benefits.

While it is very important to protect our government computers from outside hackers who break into our computers through high-tech doors, we must also look at the internal users of our computers. Experts say that most computer crime is committed by employees authorized to use the system.

To illustrate examples of this, James Huse, the SSA's Acting Inspector General, will testify, along with Ed Ryan, the Special Agent in Charge of the IG's New York Field Office. He will speak about computer crimes that SSA employees committed and how they were able to catch them.

For example, in what computer experts say may have been one of the biggest breaches of security of personal data held by the Federal Government, several employees of the SSA passed information, including Social Security numbers, date of birth, and mother's maiden name, on thousands of people to a West African credit card fraud ring. Using this information, the crime syndicate was able to

activate thousands and thousands of stolen credit cards, stealing by a conservative estimate at least $70 million. Not only was a tremendous amount of money stolen, but each person whose information had been stolen from the SSA had to personally deal with this theft. Mr. Huse will explain how they were able to uncover the crime and what SSA is doing to prevent this from happening again.

Another example of insider computer crime is what is being called virtual murder. Each and every one of us uses our Social Security numbers in our daily lives. It is something we take for granted until something goes wrong. Imagine if you went into your bank to open a new account and the branch manager said, "Mr. Jones, I am sorry. I cannot open a new account for you because our records show that you are dead." That is exactly what happened to a woman in Florida who was informed by a bank official that she was dead. It turns out that she had been communicating on an Internet chat room with a gentleman who worked for the Social Security Administration. They had a disagreement and he entered a death notice for her into the official SSA database record. We will also hear about many other ways employees who have used the Social Security Administration's computer system to commit crimes.

The final panel will be comprised of witnesses from the Social Security Administration and the VA who will comment on GAO's findings and the state of information security within their agencies. They will testify about the programs they are instituting and the steps that they are taking to protect their valuable private and sensitive information.

I will call on my other colleagues for any statements they might make.

Senator Collins.

OPENING STATEMENT OF SENATOR COLLINS

Senator COLLINS. Thank you very much, Mr. Chairman. I first want to express my appreciation for your convening this hearing on this very important issue. In this age of the Internet and the computerization of almost every record keeping function of government, computer security is a topic of utmost importance to virtually every American.

While many people tend to think of computer hackers as posing particular dangers to national security through their efforts to break into classified databases and computer systems, the computer security threat most likely to affect the health and livelihood of ordinary American citizens probably has much more to do with unclassified but private and confidential information held in ordinary databases throughout the government and in the private sector.

The Committee's hearing today will focus on just this sort of threat, taking as its case studies the danger of theft or the unauthorized alteration of private information about millions of Americans that is stored in computer archives and databases at the Veterans Administration and the Social Security Administration. These two agencies are, of course, vital parts of the social safety net that we provide for our citizens, for veterans who have served their country and for senior citizens who depend upon the SSA for

their Social Security benefits. Protecting these citizens from fraud and other abuses thus has a special urgency.

Crucially, however, as we will hear today, the VA and the SSA computer systems contain vast amounts of information about American citizens, from Social Security numbers to mortgage records, from benefit records to the most basic and private of health records.

All Americans, and especially veterans and elderly citizens, thus depend upon the VA and the SSA to have computer security systems capable of ensuring that this information does not fall into the hands of criminals or information vandals intent upon fraud or other mischief. Our hearing today will address what steps need to be taken in order to fulfill the government's obligation to provide this information security.

In addition to the well-known threat from outside hackers, moreover, I am pleased that this hearing will also deal with the significant danger of data theft by insiders, be they disgruntled employees, vengeful settlers of scores, or simply unscrupulous individuals who take advantage of their access to VA or SSA computer systems to engage in or facilitate various types of fraud. The insider threat is significantly different in some ways from that posed by outsiders, and our computer security systems need to take this fact into account.

These are, as I have noted, very important issues. However, they are not new issues. Particularly with regard to the Veterans Administration, many of these computer security vulnerabilities have been known for years and nothing has been done. This is very disturbing and it is why the leadership of our Chairman and Congressional efforts to draw attention to these matters is so crucial to the financial security and health of American veterans and our elderly.

The GAO has undertaken a searching inquiry into computer security at these two agencies, a study that included penetration testing, that is controlled break-ins to computer systems by benign hackers employed by the GAO. The study has done an admirable, though perhaps frightening, job of identifying key weaknesses.

It is my hope that by virtue of this Committee's attention, the VA and the SSA will be able to direct the necessary attention and resources to these weaknesses. In addition, it is my hope that in solving these problems at these two agencies, we will all be able to learn important lessons about how to handle computer security elsewhere in the Federal Government, and that Congress and the Executive Branch will together be able to ensure that such problems do not continue or arise again. Americans should not have to fear that confidential, private information entrusted to government agencies is vulnerable to unauthorized access and improper disclosure.

Again, Mr. Chairman, I thank you for holding this important hearing.

Chairman THOMPSON. Thank you very much.

Senator Lieberman.

OPENING STATEMENT OF SENATOR LIEBERMAN

Senator LIEBERMAN. Thanks, Mr. Chairman. Very briefly, let me join in thanking you for this series of hearings. These hearings

have been a real education for me personally, and I think they are doing a great service for our country.

I must say that I have been fascinated by what I have learned, but I have also been very discomforted by it. We are all accustomed to thinking about computers and the information revolution we have had over the past couple of decades as good and exciting developments, and, of course, they are. But as we have learned from the earlier hearings in this series, there is a vulnerable side to the cyber revolution, one that comes from the fact that we have been far quicker to take advantage of the benefits computers and networks offer and to become extraordinarily dependent on those networks before we have acknowledged and taken action to protect against the risks that dependency brings.

In our first hearing on the topic, as has been mentioned, we learned that the same advances that have made our power systems more stable, our transportation more efficient, and our information more accessible have left us very vulnerable to wider-scale disruptions of our infrastructure than was ever before possible.

In our second hearing, we learned something that in many ways was more disturbing, which is that our defense systems and our national security itself are subject to enormous threats as a result of our dependence on computers and the weak security, relatively speaking, that we have now for them.

Today, we are exploring a new aspect of this new world, which is the way in which the government's increasing automation of its information systems has left our most personal information vulnerable to exposure and exploitation. Government computers store troves of information, like medical records and wage and other personal income information, that are of great interest to voyeurs and of great value to the criminally inclined.

I must say that I was unsettled when I read the background material for today's hearing to learn how much we may have to do to provide truly adequate protection for all of this information because of how far the voyeurs and brokers and hackers are prepared to go to obtain that information.

Mr. Chairman, again, I truly appreciate your holding these hearings. I think they are illuminating the unfortunate dark side of our otherwise bright entry into cyberspace. I look forward to hearing these witnesses today and to hearing from them particularly how we can better protect ourselves from the threat posed by the problems they will describe. Thank you.

Chairman THOMPSON. Thank you very much.

I would like to recognize our first panel, James Huse, Acting Inspector General of the Social Security Administration, and Edward Ryan, Special Agent in Charge, New York Field Office of the Inspector General, Social Security Administration.

Gentlemen, welcome. Thank you for being with us. Do you have any preliminary statements that you would like to make?

STATEMENT OF JAMES G. HUSE, JR.,[1] ACTING INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, ACCOMPANIED BY EDWARD RYAN, SPECIAL AGENT IN CHARGE, NEW YORK FIELD OFFICE, OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, AND PAMELA GARDINER, ASSISTANT INSPECTOR GENERAL FOR AUDIT, SOCIAL SECURITY ADMINISTRATION

Mr. HUSE. Yes, sir. Mr. Chairman and Members of the Committee, thank you for inviting me to appear today to discuss system security weaknesses and employees who took advantage of those weaknesses to commit fraudulent activities at the Social Security Administration.

Identifying, investigating, and prosecuting SSA employees who inappropriately or criminally misuse their access to electronic records systems to commit program fraud is our No. 1 priority. We recognize that system security is a very important and very primary mission for the Social Security Inspector General's Office, as well as for Social Security itself. We all take this issue seriously. Because of our cooperative relationship with SSA, we are able to help deter employee fraud by seeking prosecution against employees who commit criminal violations and by publicizing these successful prosecutions.

I should have added at the beginning that we have submitted a formal statement for the record and this is an abbreviated oral statement for the sake of time.

Chairman THOMPSON. Your full statement will be made a part of the record.

Mr. HUSE. One of our major efforts in the detection of fraud is Operation Clean Slate, which is designed to identify and prosecute employees who fraudulently manipulate Social Security Administration's electronic records systems to commit program fraud and other crimes. Under Operation Clean Slate, we have a number of initiatives designed to identify employees who abuse the Social Security data to which they have access. Today, I would like to highlight some of those cases and projects that we have under Operation Clean Slate. I have asked Special Agent in Charge Ed Ryan from our New York Field Division to assist in the discussion of our results.

I will now turn the floor over to Ed and he is going to discuss Operation Pinch.

Mr. RYAN. Good morning, Mr. Chairman and Members of the Committee. I will provide you now an overview of Operation Pinch.

In late 1995, the Office of the Inspector General, New York Field Division, learned from the Social Security Administration of one possible corrupt employee. This fact, coupled with information received in 1996 from the Citicorp Fraud Investigation Unit informing us of a major New York credit card fraud ring led to the initiation of Operation Pinch.

Operation Pinch investigated a massive credit card fraud conspiracy orchestrated by West African crime syndicates. These criminals stole thousands of credit cards mailed to legitimate bank customers. The credit cards could be activated via a 1–800 tele-

[1] The prepared statement of Mr. Huse with charts appears in the Appendix on page 36.

phone line using cardholders' Social Security numbers, dates of birth, and mothers' maiden names as security prompts.

In order for this scheme to work effectively, the criminals enlisted Social Security Administration employees to obtain information needed to activate these stolen credit cards. A few corrupt SSA employees illegally sold identity information of 20,000 individuals whose credit cards were stolen. These West African criminals then fraudulently activated the credit cards.

Citibank, Chase Manhattan Bank, Bank of America, and NOVUS provided us additional information concerning stolen credit cards and their subsequent fraudulent activation. This credit card theft ring resulted in estimated bank losses of approximately $70 million.

I would like to now address specific cases that were part of Operation Pinch in the New York Field Division. A contact representative in Brooklyn, New York, obtained 30 Social Security account histories a day for a period of 2 years. She provided the Social Security information to a New York City Department of Social Service employee, who also was of West African descent, who then provided the Social Security information to other West African criminals who activated these stolen credit cards.

After being interviewed by Office of the Inspector General Special Agents, the contact representative resigned her position with SSA and was arrested. She was subsequently sentenced to 5 years supervised probation and ordered to pay a $100 fine.

A claims clerk in Jamaica, New York, with minimal need to access the SSA database system conducted 655 record searches during a 6-month period. After being interviewed by our special agents, the claims clerk admitted to selling 1,000 to 1,500 account records for $10 to $20 each to West African co-conspirators. She was arrested and later sentenced to 4 years probation and fined $2,000.

A local New York District Attorney obtained a search warrant for a private New York residence that resulted in the seizure of numerous Social Security records. A contact representative in the Jersey City, New Jersey, Teleservice Center was identified from the information contained in these seized records. The employee admitted to providing 100 Social Security records to a West African coconspirator for $15 per record. The employee resigned from her employment at SSA, was arrested, and later sentenced to 2 years probation with special conditions to seek psychological counseling and was fined $500.

Another query of the SSN database identified a clerk-typist at the Flatbush District Office located in Brooklyn, New York. During our interview, the subject advised that he had been approached by the contract security guard at his Social Security District Office to sell Social Security record information for $50 to $100 per record. Between November 1995 and April 1996, the subject sold Social Security records to this guard. He advised us that since the guard had only paid him $40 a record, he discontinued selling SSA records to the contract security guard. He then identified a West African co-conspirator as an individual to whom he also sold SSA records to for $50 per record during the time period April of 1996 through the end of July 1996.

This SSA employee was immediately terminated from SSA employment and was arrested for bribery. He was sentenced to 3 years probation, fined $8,343, ordered to pay restitution in the amount of $20,239 to financial institutions. Additionally, the contract security guard was barred from the SSA District Office and was terminated by the contract security service and also was successfully prosecuted.

Through SSA OIG investigations at the Flatbush District Office, a Stay-in-School clerk-typist was identified as accessing SSA records and furnishing them also to the office security guard, who worked for the West African credit card ring. The clerk-typist was terminated from SSA employment, was arrested, and sentenced to 3 years probation, 200 hours of community service, and fined $25.

SSA Office of Inspector General's Operation Pinch investigations resulted in 27 convictions to date. Of the 27 criminal convictions, 12 were Social Security Administration employees, 3 were contract security guards, 12 were co-conspirators. In addition, at this time, one co-conspirator is considered a wanted person. The Inspector General is continuing to make arrests in similar fraud cases involving Social Security fraud, including the illegal access and release of database information by Social Security employees. Thank you.

Mr. HUSE. Thank you, Ed.

Now, I would like to discuss additional significant employee fraud cases that we have investigated around the United States that are similar to Operation Pinch. In California, an SSA employee illegally sold and processed Social Security cards. The subject admitted to selling the Social Security numbers and cards for $200 each. The subject pleaded guilty to a felony count of accepting a bribe and one felony count of illegally processing and issuing unauthorized Social Security numbers and cards, and was sentenced to serve 3 years of supervised probation, 50 hours community service and was terminated from SSA employment.

In Kansas City, Missouri, in another case, the subject, a Social Security employee, had accessed and changed Social Security records pertaining to herself and family members, resulting in the issuance of unauthorized checks to 10 deceased beneficiaries and two living beneficiaries. The subject changed the addresses of these beneficiaries to reflect her own address and her friends'. Then the subject conspired with another Social Security benefits authorizer and had the checks issued to herself, her husband, her son, and her friend. The amount of fraudulent checks involved in this particular instance totaled $174,312. One subject was ordered to serve 15 months in prison, 3 years probation and pay SSA restitution of $174.321. The other was ordered to serve 5 years probation and pay restitution to SSA in the amount of $20,933.10.

In Chicago, a benefits authorizer at the Great Lakes Program Service Center generated "one-check-only" payments to fictitious individuals by entering false data into the records of existing beneficiary accounts. These checks were then direct deposited by false entries into the personal account of this particular employee. Again, the subject plead guilty and was sentenced to 1 year incarceration and ordered to pay SSA $7,200.

In Florida, a claims representative improperly and maliciously changed the Social Security card of an individual, and this is the

case alluded to by Senator Thompson, so I will pass over that one. That is the virtual murder case.

In another Florida case, a Tampa, Florida, based company was selling confidential government information, including detailed earnings queries and Social Security number queries. This investigation uncovered that this company had suborned a Fort Lauderdale Social Security teleservice center representative who accepted bribes from that company in order to provide them with the data that they required for this business process. For his services, this Social Security employee was paid $3,000. Subsequently, that employee plead guilty and was sentenced.

Now, Mr. Ryan will describe one more case in New Jersey that is significant in this respect.

Mr. RYAN. Thank you, Mr. Huse.

Another significant employee fraud case involved a Social Security Administration benefits authorizer. In March of 1995, the Social Security Administration regional security staff in New York received a referral from a small New Jersey bank regarding suspicious activity in a customer's account. We, in coordination with the Administration's Northeastern Program Service Center integrity staff, determined that an SSA benefits authorizer in New Jersey made a number of SSA electronic transfers in the amount of $2,999 each.

The investigation concluded the benefits authorizer fraudulently established SSA payments not only to himself but others and then diverted approximately $328,731 from March 1994 through March 1995 by electronically depositing the fraudulent funds into these accounts. The co-conspirators were not SSA employees and they were not entitled to receive these funds.

The benefits authorizer resigned his position at SSA, was arrested by OIG on charges involving wire fraud and money laundering. He was later sentenced to 4 months imprisonment, 4 months home confinement, 3 years supervised release, restitution of $50,000, and a special assessment fee of $50.

I would like now to turn it back over to Mr. Huse.

Mr. HUSE. To conclude this, Mr. Chairman, employee fraud cases represent the smallest number of cases we investigate in the Inspector General's Office. However, we have made employee fraud our primary mission. We believe, along with the Commissioner and the executives of the Social Security Administration, that employee fraud is a serious matter that must be dealt with effectively.

We believe that successful prosecutions are a key deterrent against employee fraud. We publish these cases throughout the agency in cooperation with Social Security Administration highlighting these effective prosecutions. In this way, prosecutions are made public and all Social Security Administration employees are made aware of the fact that Social Security Administration has a zero tolerance for fraud. We are dedicated to eliminating employee fraud and misconduct at SSA and I wish to thank the Committee again for focusing on this important and serious issue.

I would be pleased, along with my staff, to answer any questions you may have at this time.

Chairman THOMPSON. Thank you very much, gentlemen, for your information. In many respects, perhaps we are calling you out of

sequence because you show what can happen on the tail end as a result of your investigation and bringing people to justice with regard to some of these things, but you can help us deal with what causes this in terms of weaknesses in our system and what we might do to rectify it. Obviously, you are going to have people in all branches of government, as well as private life, who, from time to time, are going to violate the law and figure out ways to game the system.

I guess what I come away with initially is how easy it seems to be. You have rather low-level employees who can enter into conspiracies with outside people in order to furnish them information, who can go into the computers and pay themselves benefits if they want to. You have 12 here.

I think it is also instructive as to how these cases were made. It seems like they were not made by managers within the Social Security Administration. They were not detected through whatever procedures they might have to detect such things. But, rather, I think they started out with bank investigators who noticed some suspicious circumstances, did they not? How did that come about?

Mr. RYAN. That is correct. In one case, we did have information from Social Security Administration from doing audit trails of one possible corrupt employee. After about another 3 months is when we began to get the referrals from the credit card financial institutions and it turned out to be the same employee originally referred to us by the Social Security Administration.

Chairman THOMPSON. So is that what started the entire Operation Pinch investigation? Is that how that came about?

Mr. RYAN. Investigation of the one, coupled with the 1996 updated information from the financial credit card issuers.

Chairman THOMPSON. So I believe the bank investigators noticed an increase in stolen credit card activity and reported it through the Secret Service to the Social Security Administration IG, is that correct?

Mr. HUSE. That is correct. The case had two prongs, if you will, in terms of its origin. We received early information that there was some employee activity that required investigation, and then coupling that with a later notification by the financial community of credit card activations that they suspected had to come from some information that would have come from our databases caused us to put the two together and then focus on the crime.

Chairman THOMPSON. Do we know how many files were involved, how many pieces of information or how many citizens' records were violated? You are talking about 27 convictions including 12 SSA employees, do you have any damage assessment from that standpoint?

Mr. RYAN. From the number of credit cards and the financial losses estimated by the credit card companies themselves, it would probably be approximately 20,000 records.

Chairman THOMPSON. Twenty-thousand records?

Mr. HUSE. That is 20,000 records that we, from our interviews of these suspects, have determined as well as we can that they passed over to these conspirators. We cannot really link that exactly to the number of credit cards that were activated because in addition to suborning our employees, these sophisticated conspir-

acies also tap other databases, to include those of the very financial institutions that were defrauded here. So it is a mix there. There is not a direct correlation. We know that 20,000 records were passed to these people, but how many of them were in these cards, the financial community is circumspect about providing us exactly with that information for obvious reasons. That is bad advertising for them.

Chairman THOMPSON. Right. So you know at least 20,000 records were violated, and we do not know how many other records from other sources that this conspiracy might have gotten into. And, of course, you know, the first thing that occurs to you is that there are lots of other potential conspiracies out there and the question is, how do we know? There are 20,000 records by a handful of low-level employees, typists in one case, who are being, in effect, used by an outside conspiracy.

Do you have any indication that there are other groups, sophisticated or otherwise, out there who are making attempts, that you do not have cases yet, and I will not ask you the details of your investigation, of course, but do you have other indications of attempted penetration in that regard?

Mr. HUSE. What we have done, and that is a very good question, we are a relatively new agency because we came into being with Social Security's independence. In the last several years with considerable resources that we have been given by the agency, we have been able to develop a capacity to deal with this, what I would call intelligence information about emerging financial crimes, conspiracies, and you are absolutely right, there are many.

We have a Strategic Enforcement Division that does nothing but focus on these types of crimes. We have a new memorandum of understanding with the agency that gives us tremendous access to the agency's databases in order to monitor any kind of what we believe is an emerging investigative lead, so that with rapid deployment of our investigative resources, we can get on something like this as soon as we get the tip.

We have a strong relationship now with the credit card and financial community so that we exchange information about emerging trends and patterns. All of this has come to pass as a result of Operation Pinch and the lessons learned.

Chairman THOMPSON. You are addressing your capabilities, and that is good information. My question has to do with what you are doing with those capabilities. Is it too early to tell yet, or are there other indications of attempted penetrations by other groups?

Mr. HUSE. We can tell that on the cases that come to our attention that we are able to rapidly get out there—and we have a number of employee cases, but the number is extremely small in terms of the overall number of cases we have in our inventory. I would say that, although there are these attempts, they are not in significant numbers at this time.

Chairman THOMPSON. All right. In our past hearings, experts have made the point that good security practices are as much a matter of management practices as they are a technical problem. You apparently have a pretty good technical system in place for tracking suspicious computer activity, so I am puzzled why these audit trail reports never alerted the relevant managers to sus-

picious activities in the Operation Pinch cases. Would not reports have shown suspicious spikes in computer browsing by the employees? Are managers paying enough attention to the audit reports that they are getting?

First of all, you might describe these audit trails, in the first place, and then second, should they not have alerted managers more readily in these cases?

Mr. HUSE. You are entirely correct that that is on the front end of these cases. We have done—that is outside of the investigative arena, that is more on our audit side, and if you will permit me, I would like to call up our Assistant Inspector General for Audit, Pam Gardiner, who will speak to some of our audit work in this respect, and then I am sure the agency also has some——

Chairman THOMPSON. Welcome. Would you state your name for the record, please?

Ms. GARDINER. Yes. Good morning. I am Pamela Gardiner. As far as the audit trail system goes, it captures so much data that it is primarily used by the Social Security Administration after the fact, when an individual is identified as having committed a crime. SSA can go back and review every transaction that has occurred with that person.

In our audits, we have made a number of recommendations through the years. The agency issues an annual accountability report, and in these reports we have identified separation of duties, in particular, as a significant weakness. The agency has problems with separation of duties because of downsizing and they have to allow employees to do more than they used to in the past because they have fewer people to process more transactions.

So our main emphasis has been on compensating controls that they should implement, and the audit trail system is one. It could be improved. When certain high-risk transactions occur, an employee puts in his/her password, but then we suggest that a supervisor also put in a password before that transaction can actually take place and be implemented. We call that a 2–PIN process.

We also suggest that employees have the most limited amount of access to systems as possible. It is a concept called least privilege, where an employee should only have access to those systems that they absolutely must have access to in order to perform certain transactions.

And then finally, as far as the audit trail system, what we are going to recommend is that, right now, the system does not have what you would consider to be measurements or matrices that would identify things like employees should process so many transactions an hour or certain types of transactions, and when those numbers go way out of whack or beyond what is normal, a flag would appear and that way they could really focus——

Chairman THOMPSON. The system that you have now—does not each employee have a unique PIN number?

Ms. GARDINER. Yes, they do.

Chairman THOMPSON. And your computers generate audit trails that can show where employees have looked into databases of personal information? Do you not have that availability and capability?

Ms. GARDINER. That is correct. Yes.

Chairman THOMPSON. That being the case, you are saying, basically, that the audit trails are useful in solving crimes but not much in preventing crimes. Is it because you do not have that information, that it is not being kept the way it should be, or that it is not being used by managers the way perhaps they should be using them on the front end to analyze and see who is looking at what? That would not be total prevention, because they have already looked, but certainly it may be before things get out of hand.

Ms. GARDINER. Right.

Chairman THOMPSON. What is the problem there?

Ms. GARDINER. Several. One is that there is so much information. There are so many employees and so many transactions on a daily basis——

Chairman THOMPSON. It is so voluminous that managers just are overwhelmed with the load of information and they wind up maybe not using it as much as they should?

Ms. GARDINER. Well, they try and do samples and look at certain things, but again, it is an awful lot of information. Also, managers do have other high-priority work and so they cannot always get these reviews in and do everything else. So, there is a little bit of inconsistency in how often they do the reviews.

Chairman THOMPSON. Mr. Huse, did you have a comment on this?

Mr. HUSE. I was going to say that there are also some planned enhancements that we believe are going to be very effective that the agency has invested in that are pending, that will help in this audit process, but those are not on-line yet. They call it CHIRP. It is an acronym for basically this kind of review of these audit trails.

Chairman THOMPSON. You are talking about the problem being a continuing one of employees selling information. Did you mention that the New York IG Office just arrested several more employees in connection with another fraud ring? Is that true?

Mr. RYAN. Just recently?

Mr. HUSE. Not recently, but we have these cases occur infrequently, and that is very important, that this is not an epidemic issue. This is an issue that I think we react to very quickly. These recommendations that we have made are before the agency and the agency is probably best suited to answer exactly how they work with those.

Chairman THOMPSON. Are you making recommendations such as additional training and things of that nature for Social Security Administration employees in terms of using the data that is available to them?

Mr. HUSE. We have made those recommendations in a general sense in the work on our audit site. In addition to that, we participate with the agency in a national anti-fraud effort, and in that, the training and the raising of the profile of security in terms of our employee awareness is a major imperative inside Social Security Administration.

Chairman THOMPSON. There is at least one criminal statute against improper use of Federal Government computer data. Do you think that the existing laws are satisfactory or sufficient to deal with the problems that you are running into?

Mr. HUSE. I am glad you raised that, Mr. Chairman, because I think we have a good Federal law but it could be a little bit better. One of the problems we face, as you can see from our statement on the record, is that a lot of times, the actual sentencing for these particular crimes is not what it could be.

Chairman THOMPSON. Yes. I noticed that out of all that, I do not think there was 1 day in jail.

Mr. HUSE. For many people, there is not.

Chairman THOMPSON. That first one, you mentioned a $100 fine?

Mr. RYAN. A $100 fine.

Chairman THOMPSON. A $100 fine and probation. Well, that will put the fear of the Lord into them. [Laughter.]

Mr. HUSE. Right now, in the Federal computer crime statute, 18 U.S.C. 1030, there is a monetary threshold that has to be met for the gravamen of that offense to attach for potential prosecution. We often cannot get there. It is very difficult sometimes for us to take what has happened——

Chairman THOMPSON. Because you catch them before they reach the amount sometimes?

Mr. HUSE. Right, and that prevents sometimes the interest that could be there, if there were a different standard, if we could change that statute to make the access itself or the theft of the information the graviment of the offense.

Chairman THOMPSON. Some question has been raised, too, as to whether or not it sufficiently covers the employees from accessing data within their own department.

Mr. HUSE. That is correct.

Chairman THOMPSON. I think most of the statutes have to do with outsiders coming in.

Mr. HUSE. Correct.

Chairman THOMPSON. Perhaps that needs to be looked at and tightened up some.

Mr. HUSE. I am not certain of the bill's number, but I know Senator Kyl's bill does put that bite in it in terms of identity fraud theft, for that type of data, and that would be a significant help for us itself.

Chairman THOMPSON. We have had coverage there for disclosure of information. I think we are just now getting into the damage that can be done just——

Mr. HUSE. With the data itself.

Chairman THOMPSON [continuing]. By accessing it. Of course, we just passed as part of the IRS bill a criminal provision for willfully inspecting tax returns, but that is limited to tax returns.

Mr. HUSE. That is the browsing aspect.

Chairman THOMPSON. Yes. That is the browsing aspect. So we are gradually getting there, I think, as we see what all is going on out there and what is being done with these records. You deal with tax matters, too, but you deal with a lot more matters than that.

We have three panels today, so I am not going to keep you any longer, but obviously, you have done some excellent work here. Keep it up, and thank you for coming today. I appreciate it.

Mr. HUSE. Thank you.

Mr. RYAN. Thank you.

Chairman THOMPSON. We will proceed to our second panel, Gene Dodaro, Assistant Comptroller General, Accounting and Information Management Division, U.S. General Accounting Office; Robert Dacey, Director for Consolidated Audits and Computer Security Issues, Accounting and Information Management Division, U.S. General Accounting Office; and Keith Rhodes, Technical Director for Computers and Telecommunications, Accounting and Information Management Division, U.S. General Accounting Office. What do you gentlemen do when people ask you what you do for a living? Certainly, you do not take the full 5 minutes to go through your title. [Laughter.]

Mr. DODARO. Basically, Senator, I tell them we get to audit the IRS.

Chairman THOMPSON. All right. People understand that, and they probably give you a standing ovation. [Laughter.]

Thank you for being here. Is there any preliminary statement that you would like to make?

STATEMENT OF GENE L. DODARO,[1] ASSISTANT COMPTROLLER GENERAL, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY ROBERT F. DACEY, DIRECTOR FOR CONSOLIDATED AUDITS AND COMPUTER SECURITY ISSUES, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE, AND KEITH RHODES, TECHNICAL DIRECTOR FOR COMPUTERS AND TELECOMMUNICATIONS, ACCOUNTING AND INFORMATION MANAGEMENT DIVISION, U.S. GENERAL ACCOUNTING OFFICE

Mr. DODARO. Yes. Good morning, Mr. Chairman. We are very pleased to participate in the series of hearings being held on information security. The attention you are focusing on this important subject is providing an important stimulus for needed improvements.[2]

Since GAO identified information security as a government wide high-risk area in early 1997, several encouraging developments have transpired. First, agencies are beginning to pay more attention and respond more favorably to recommendations by auditors. We have worked to build into the Chief Financial Officer Act annual audit requirements a detailed look at computer controls, and that has helped provide incentives because you have an annual report card every year.

Second, based on our recommendation, OMB and the Federal Chief Information Officers Council have designated information security a priority area for the government. And last May, as you know, the President issued the directive to improve the critical infrastructures of the Nation, including the Federal Government's infrastructure.

Now, all these activities are stimulating increased attention, but there is a great deal more that needs to be done to develop and maintain an effective security program for the Federal Government. As you mentioned in your opening statement, we are releasing a report today done at the Committee's request that details the

[1] The prepared statement of Mr. Dodaro appears in the Appendix on page 54.
[2] GAO report submitted by Mr. Dodaro appears in the Appendix on page 85.

serious weaknesses in the 24 major departments and agencies of our Federal Government. Those departments and agencies cover virtually all the revenue collection activity of the government as well as virtually all the expenditures that are made on behalf of our National Government.

These pervasive weaknesses include poor access controls over sensitive data, incomplete and untested plans to require continuity of services in the event of disruptions, and inadequate organization-wide planning and management of security programs. Until these areas and specific weaknesses are rectified, critical Federal operations and assets are really put at risk. As has been pointed out today, the Federal Government's exposures to individuals and groups inappropriately accessing sensitive data, or modifying computer programs for personal gain or sabotage remains an extreme risk for the Federal Government.

Now, two agencies that you are focusing in on today, VA and the Social Security Administration, illustrate the type of risk that can occur and also what actions are required to fix these problems. Our audit at the VA, for example, uncovered the fact that thousands of authorized users at the VA had much more access to read and change files than was necessary. Additionally, user identifications and passwords controls were weak. Passwords were often shared among employees or easily guessed, and people who had been terminated by the VA or transferred to another department were not removed promptly from authorized lists of users.

This greatly increased the risk of several things occurring. Payments for payroll and other financial transactions could have been altered. Also, it increased the risk that sensitive medical records, including diagnoses for illness as well as treatment that had been received by veterans, could have been viewed or disclosed. Similarly, information on the veterans' home mortgage program, such as default rates and delinquencies, could have been disclosed or were readily available for people to view.

Our penetration test at Veterans Affairs also disclosed that we were able to easily gain access to its mainframe and network computers, and with this access, we could have modified information in the loan guarantee program, which is a multi-billion dollar loan portfolio. We also could have had access and modified, deleted, or destroyed information on VA's sensitive programs in veterans' compensation, pension, life insurance programs, as well.

These weaknesses were further exacerbated because VA did not have an active monitoring program to review trends in access information. This is similar to the issue that you were asking Mr. Huse earlier, who is monitoring the activity of authorized users or others entering into the systems, and we found that to be a weakness at VA.

Similarly, at SSA, weaknesses were noted by auditors there, as well. User identifications and passwords controls, again, were very weak and easily guessed. Additionally, penetration tests at VA allowed auditors to gain access to systems that would have enabled them to view sensitive data and destroy that data, and add or delete users. This puts information such as sensitive information on Social Security numbers, earnings statements, and benefit payments at risk. It also creates the opportunity for people to create

fictitious beneficiaries, as well as basically steal some of the information and sell it for personal gain.

Now, both at VA and the Social Security Administration, numerous recommendations were made to fix the individual weaknesses that have been identified. Also recommendations were made in both agencies to put in place a comprehensive security management program. As you recall, in May, the work that we had done for this Committee on the best practices of leading organizations that have good information security programs led to the publication of this report. In this report, we outline the conclusions of the lessons learned from people who do security well. That is you need a central focal point to focus on this activity, you have to assess risk, you have to monitor, and you have to raise awareness of the employees, as you pointed out in your earlier questioning of the witnesses, and you need to monitor and evaluate and test the systems in place. This type of comprehensive security program needs to be put in place in every organization in the Federal Government.

Chairman THOMPSON. When did that come out?

Mr. DODARO. That came out in May, Senator. We had an exposure draft issued earlier. This guide, in addition to being endorsed by this Committee, has been endorsed by the Federal Chief Information Officer Council. We are consistently working with the CIOs and the Inspectors General and others, to put this type of process in place.

In addition, in the report we are releasing today, we have recommended that OMB work with the National Security Council to have a government wide, comprehensive strategy, emerge from their efforts. We know that plans are underway. We have not yet been able to review those plans. They have not been made available. We will plan to review them and apprise the Committee of our conclusions about whether or not this comprehensive strategy has emerged. Central management is needed in addition to the individual agencies fixing their problems to follow up, deal with government wide cross-cutting issues, and really monitor whether or not the agencies are making progress.

Chairman THOMPSON. Through OMB?

Mr. DODARO. Yes. OMB has the statutory responsibilities, but also the National Security Council now, under the President's directive that was issued in May, is launching a major initiative that involves the private sector, State and local governments, but also the Federal Government. One of the goals of that directive is to make the Federal Government the "best practices" example of information security to show others in the private sector, and there is a lot that needs to be done to be able to achieve that goal.

Whole information security is a continuing concern, there is really one caveat I want to emphasize here this morning. Over the next 18 months, as organizations grapple with the year 2000 computer conversion, information security needs to really be given heightened awareness. At no time in our history are so many computer systems going to be modified at the same time, thus increasing the risk that security could take a back seat. The year 2000 computer conversion is the most dramatic example yet of the dependence that we have as a Nation on our computer systems and how vulnerable we are to potential disruption. So that really needs to be

given a lot of attention. We have emphasized this to OMB and the agencies and special focus is needed over this next couple-of-years period.

But such challenges in information security are not going to end with the new millennium. They are going to continue in the future. There needs to be long-term programs put in place. We at GAO are committed to work with this Committee and with the Executive Branch to make sure that happens to reduce our vulnerability and risk.

That concludes my opening statement, Mr. Chairman. My colleagues and I would be happy to answer any questions.

Chairman THOMPSON. You are talking about the Y2K problem. It certainly fits right together with the subject we are dealing with today, as you point out, and my understanding is we are having to bring in thousands of people from other countries to address our Y2K problem. We just do not have the manpower, and that in and of itself, of course, raises serious security concerns because we do not know if we have been the victim of sabotage, for example, until sometime after the fact. It is just an additional avenue that those who would do us harm are going to have, in addition to all the others that we have had, is that correct?

Mr. DODARO. That is correct, Senator. I will ask Keith to elaborate in a minute, but there are two basic risks, one that you point out, in that fixing the software problems there could be shortcuts that could be taken in order to get the work done on time. As you well know and we have reported, many Federal agencies are way behind in fixing their problems. Some of the organizations in the private sector are behind, as well. It is an international problem globally.

So a lot of people are under a lot of pressure, and as you have heard, one of the reasons we are in this information security dilemma of being very vulnerable is that information security has always taken a back seat to getting the systems developed and put on line quickly, and there is tremendous pressure now.

The other big risk is that if something occurs during that period of time, one would not know or could have difficulty distinguishing between a year 2000 computer failure and whether or not somebody is intruding into your system and trying to do malicious harm to that system. But Keith has been focusing on the year 2000 problem and has a very good perspective on that.

Chairman THOMPSON. Will you elaborate on that for us?

Mr. RHODES. Just to expand on what Mr. Dodaro has already said, by its very nature, since everyone is late, everyone has to focus on what is mission critical. Now, by that very definition, you are exposing yourself to letting everyone know what the crown jewels are.

Now I am turning it over to a contractor which I have brought in at the 11th hour because anyone who got started early already sucked up the resources necessary. That contractor will then subcontract and subcontract and subcontract, or I will just take my code and give it to—one of the big software houses in the world right now is India. A little while ago, they set off a nuclear weapon that upset a lot of people. They are very good coders. I do not know

that somebody in a foreign country can necessarily get the security clearance that I would want them to have.

Recently, I read about George Soros, the entrepreneur, wanting to bring the Bulgarians over from the Bulgarian Virus Institute because they are very good code writers and have them work on our code. When I was working in national security prior to coming to the General Accounting Office, a lot of my time was spent fighting the Bulgarians that are now going to come in and fix our code.

From my perspective, not necessarily being labeled an aging Cold Warrior or something, I do not necessarily like to bring my former enemies in to fix my code. But people are in a position of being desperate and now they open the flood gates and say, well, I absolutely have to fix my system. As we see, as your hearings point out, security is not a top priority for a lot of organizations.

Chairman THOMPSON. It is not now, and it is going to be even less, in and of itself, as they face this crisis.

Mr. RHODES. Absolutely.

Chairman THOMPSON. If they are going to be manufacturing automobiles or widgets or whatever, that is going to be their prime concern.

Mr. RHODES. Right, and in the year 2000, not just from a government perspective but from the entire infrastructure perspective, you are talking about power, you are talking about water, you are talking about telecommunications, you are talking about emergency services, you are talking about traffic lights, you are talking about elevators, and you are talking about your business codes, so you are having to open up everything.

The year 2000, like security, is a horizontal issue. It cuts completely across the organization and touches everything that you, by your own definition as the chief executive officer, declare to be mission critical. Now you have given your opponent, so to speak, all of the information she or he needs to figure out where your heart is.

Chairman THOMPSON. As you say, there are three completely different, in a way interrelated but different, avenues into our most critical systems: Transportation, communication, and finance.

Mr. RHODES. Right.

Chairman THOMPSON. That is a very troubling way of looking at it. People are now focusing on the Y2K problem more and more. What you are pointing out here in these hearings is that we have this other existing problem. You, obviously, have been able to walk into the VA and get whatever you want. I mean, any amateur—we had a bunch of kids—I call them kids, I guess I am old enough to call them that—very young men come in in one of our prior hearings. They said, we can shut this place down if you give us a few hours and what not.

You, obviously, especially with the VA, were able to get access to any information that you wanted to and you could wreak havoc with that, and to a lesser extent with the Social Security Administration. We picked those two agencies, for example, because these were agencies that you had dealt with and had made an assessment of in recent times. We were not just singling them out, but that you happened to have made assessments of those two in recent times, and it is pretty clear.

We can talk about details, but anyone with any sophistication can get into pretty much whatever they want to. It is a continuing disaster waiting to happen. It is nothing that cannot be handled if we get on the job, but that is the question. Are we on the job? For example, in the Veterans Administration, this problem has been pointed out and around for some time now.

Give us some assessment agency-wide or government wide. How long have you been dealing with this? Obviously, we have, hopefully, heightened the level of attention a bit with the hearings that we have had, but how long have you been on the case? How long have these agencies been told, at least, that they have got major problems? I will stop there.

Mr. DODARO. It varies by individual agency. For some, there have been reports for many years, as was pointed out with VA. What we did at GAO is we put computer security as a high risk across the government in early 1997. We also put year 2000 computer conversion on a government wide high-risk list at that time, as well.

Chairman THOMPSON. And when was that?

Mr. DODARO. That was in February 1997, and we had issued reports earlier than that. A lot of this attention we have been able to generate actually through the requirements in the Chief Financial Officers Act, which is another management statute passed by this Committee. For those annual financial audits now, we examine and have developed methodologies to look at, computer controls over those financial systems and sometimes that leads us into non-financial systems, as well. While some of those audits date back to the early 1990's, in 1996, all 24 departments and agencies were required to now have an annual audit.

That annual audit requirement means getting a report card every year, as opposed to doing an audit in one part of an agency 1 year and going back 3 years later. That annual requirement is really putting more pressure on the agencies to make the changes and I think it is having an effect. Awareness is increasing due to these hearings this Committee has had and other pressures that we are trying to generate through these audit requirements. Agencies are beginning to take action.

Chairman THOMPSON. GPRA requirements, also, hopefully, will help along those lines.

Mr. DODARO. I agree, Senator. This focuses attention on performance as well as accountability, which is basically the heart of those statutes. We are starting to see more awareness, more responsiveness to recommendations, but it has to be more than a reactive posture on the part of the agencies. They have to take this comprehensive, proactive look at security, make it a top management priority, and make it part of the fabric of managing the agency.

Chairman THOMPSON. But they are not going to do that until they are told to do that, and the people to tell them to do that is the administration, and the arm of the administration is the OMB. Now, what has happened since this Presidential directive has come down? What specific action has been taken from a government wide standpoint since the Presidential directive came down?

Mr. DODARO. I will ask Mr. Dacey to elaborate, but there are some plans that have been put in place and they have some goals, but it has not evolved very far.

Mr. DACEY. The PDD63, as it is called, really set in motion some organizations to deal with the issue. There was a National Coordinator for Critical Infrastructure Protection that was created, including—he is also chairing another committee which is made up of agency representatives in terms of dealing with their critical infrastructure problems, including computer security. There is also another goup that was formed in the Department of Commerce, the Critical Infrastructure Assurance Office, as well as a department within the FBI on investigating some of these issues.

Thus far, not a whole lot has been done in terms of getting well down the road. Some initial actions have been taken. In response to our report, the OMB did tell us that, in fact, they are coordinating with this group to come up with this combined strategy that Mr. Dodaro referred to earlier, but as he said, we have not seen that plan so cannot really comment on it at this time.

Mr. DODARO. Mr. Chairman, in September 1996 we issued a report calling for OMB to take a more aggressive posture in this computer security area, right before we put it on the high-risk list. OMB has taken some action along with the Chief Information Officer Council, but we reiterate in our report being released today that there has to be more action on the part of the central management agencies to make sure that action is taken across the board in the government.

Now, OMB believes that this is an important issue, but also believes that the responsibilities lie at the agency level. We agree with that, but we are also saying there needs to be more action at the central management agency. You need both. It is not one or the other situation.

Chairman THOMPSON. Well, it is obvious to me. I am not going to ask you to pass judgment on it further, but the OMB has not responded to this the way that they should have. I mean, they clearly do not see it, apparently, as being that big of a problem. The President issues a directive and gets some headlines out of that, and then when you ask the question, what has been done pursuant to that, well, they have had a study group and a commission and some people have met and we are on the case.

There is not one tangible thing that I can see that has been done, and you have been onto them since 1996 now, not one thing from a government wide standpoint has been done to highlight this problem and to instruct people as to specific things that are expected out of them in these agencies. I might add that it seems mighty similar to the Y2K problem. Until recently, I mean, Congress has practically had to drag them kicking and screaming into addressing that, and now they have got Mr. Koskinen over there with a handful of people and he is apparently going to be assessed the responsibility for transforming the government overnight, and that is not going to be done, either.

So you have a couple of disasters there waiting to happen, but it might be on somebody else's watch, but it is not good government. It is not right. You need to keep doing what you are doing and highlighting these problems and pressing them, as I assure

you we will, to take their responsibilities. We get so caught up in the day-to-day that we are not really sufficiently addressing the problems. I would not even call them longer-term problems. They are going to be here before you know it.

I have been amazed. I mean, I am glad that we can have this public hearing. We are just talking about what we can disclose in public. There is a lot of information here we cannot disclose in public. We are on borrowed time. We have been told by the FBI Director in public session that we are in for a long drawn-out battle as far as terrorism is concerned. It is amazing that we have gotten by as well as we have in terms of some of these problems, and I guess we are going to have to have a disaster to get anybody's attention, but let us hope not.

I do not know how much detail we need to get into as to what you have been able to do. I mean, access seems to be fairly complete. We talked about the technical problem versus the management problem, or insufficiency of resources as to where to assess the responsibility for poor information security. As I understand it, the Social Security Administration has a security management program that does not seem to be working very well, and the Veterans Administration has no security management program at all, is that correct?

Mr. DODARO. There are issues with both of the organization-wide plans. I will let Bob elaborate on both of those. The biggest problem in the Social Security Administration, as you heard this morning, was the unrestricted access by the employees in a large organization like that. There are dimensions of both at VA. Problems with broad access of employees within VA as well as vulnerabilities to outside intrusion, but I will let Bob elaborate on those.

Chairman THOMPSON. While you are on that point, either you or him, what do you recommend with regard to that? Clearly, a large number of employees have got to have access to a lot of information.

Mr. DODARO. They have much more access than they need. One of the things that we found is that people who had left the agency months ago were still on the rolls as authorized users and could have logged into the system. So as soon as somebody leaves the agency, it is a very simple technique to remove them from lists of authorized users.

Second, Senator, we recommend that they periodically review how much authority people really need. A lot of times they are just given broad access without any periodic reviews. People change jobs. They change responsibility. So a management focus needs to be put in place, and so we have had a number of recommendations. The auditors at Social Security have made those recommendations, as well, and they have detailed dozens of specific recommendations to address those issues. The solutions are well known. It is the management commitment and the follow-through that need to be put into place.

Chairman THOMPSON. That is the point, is it not?

Mr. DODARO. Yes.

Chairman THOMPSON. Mr. Dacey, did you want to comment on the VA part?

Mr. DACEY. In terms of the VA, they have some controls there, but overall, they do not have a comprehensive program for security management, and as a result, these kinds of things that we found in the audit are not identified by management and fixed.

Chairman THOMPSON. Do we know of any other agencies that do not have a comprehensive security management program?

Mr. DACEY. We found in doing our work, where that area was reviewed, that there were significant weaknesses in every agency's computer security management program.

Chairman THOMPSON. That does not really answer my question. My understanding was that there was no management program as such, no security management program as such with regard to the VA.

Mr. DACEY. They do not have an overall program. There are some pieces that may be better controlled than others, but overall, they do not have a strategy or program to make sure all the pieces fit together in an integrated fashion.

Chairman THOMPSON. How many do you know? I do not know if you have assessed it all or not, but are there other agencies in that same situation, other than the VA?

Mr. DACEY. There are other agencies that do have similar problems to VA's.

Chairman THOMPSON. No overall comprehensive program?

Mr. DACEY. That is correct.

Chairman THOMPSON. They have bits and pieces, but no program as such?

Mr. DACEY. That is correct. SSA is one agency that does have an active program. It just did not cover all the aspects or deal with some of the minor issues.

Chairman THOMPSON. Do you know how many other agencies? Could you give us some estimate?

Mr. DODARO. Senator, in our report, we talk about the need for entity-wide security program planning and management. We found in the audits, where there are 17 of the 24 agencies that this aspect was reviewed, all had deficiencies in their programs. So while some have more programs than others, of the 17 of the 24 where this was reviewed, all 17 had some deficiencies in their organization-wide planning and management activity.

Chairman THOMPSON. I am trying to get into a quantitative difference and maybe it merges so much you cannot make the distinctions I am trying to make. It seems to me to be a different situation to have a deficiency in your program than not having a program.

Mr. DODARO. Right. I understand what you are saying, and I do not think the reviews we did specifically answered your question like that.

Chairman THOMPSON. All right.

Mr. DODARO. The best answer I can give you is that the deficiencies that are noted are serious ones, which means they have a major element of their program missing, and it is not just a nuance.

Chairman THOMPSON. This is not news to them that they have these deficiencies?

Mr. DODARO. In most cases, it is not news. One of the things, though, that has really driven home this point is the fact that we started doing what is known as penetration testing, as you mentioned. Before, we had talked about the fact that agencies had weaknesses and vulnerabilities, but they did not really believe it, so we were able to now sit down with the tools that are available and the people that we have hired and go in and actually show them how we can enter their systems.

Chairman THOMPSON. How long would it take you to train an amateur, just anyone with just rudimentary or hardly any skills at all, using the tools that you had to hack into these computers?

Mr. DODARO. I will ask Keith or Bob to elaborate, but it would not take very long. A lot of these are well-known tools. Most of the hackers are self-taught over a period of time. There are also techniques where, with the auditors, we have used techniques called social engineering where all you do is call somebody up over the telephone and tell them you would like to have a password to get into their system. You are able to persuade them to give you that information over the telephone. This requires no technical training, and some of the other software tools are so automated now in terms of automated dialers that can go through until you can hit and dial in on a modem, but I will ask Keith to elaborate.

Mr. RHODES. I could turn you into a hacker with one keystroke. That is how long it would take, if I had the right tools. I would bring it up on your computer and say, Senator, put the mouse here. Click that button and it will go, because the tools have been automated. They have put a nice front end on them. I can sit down. Some of them are very stealthy. Some of them are very noisy. But it is a matter of you do not have to be a rocket scientist to break into systems anymore.

Chairman THOMPSON. Also, I believe the VA does not have a monitoring system, is that correct? So that if someone gets in there, they can stay forever, presumably, because there is no monitoring. Explain the problem with that.

Mr. DACEY. The situation is similar to the one we talked about in Social Security in the prior panel. They do not have a process to really identify unusual or suspicious activity taking place, either by employees who are exceeding their authority or by others who are trying to break into the system. The incidents when we did our penetration testing were not detected by other systems and this is one of the major weaknesses that we report in our report to them.

Mr. DODARO. This is one area, too, Senator, like, for example, the IRS browsing situation that you mentioned that led to the legislation to have criminal penalties. For years, IRS did not have in place a system that effectively allowed them to monitor that type of activity, so that is a fairly common problem. That is one element of this comprehensive plan that we are trying to get organizations to put in place and it is sorely lacking in many organizations.

Mr. RHODES. This also illustrates a point where the technology intersects with the management, because you can have tools that assist you in doing the monitoring, but you have to understand what thresholds you are looking for and that is a management consideration, so you have to understand what is too much authority, what is too much activity, and that is going to be an operational

definition that comes from the managers as opposed to the technology.

Chairman THOMPSON. All right. Well, listen, you have made a major contribution simply by this report here, which I hope a lot of people will read because you set out in detail the weaknesses. I think the title says it all, "Serious Weaknesses Place Critical Federal Operations and Assets at Risk".[1] We thank you for that. This is clearly a continuing matter that we want to continue to work together with you on and we admire your straightforwardness and competence, as always, in these matters, in highlighting these serious problems that we face.

Unless you have any closing comments to make or observations, I will thank you for being here again today and express our appreciation for your work.

Mr. DODARO. Thank you, Senator.

Chairman THOMPSON. Thank you very much.

We will proceed to our third and final panel, Harold Gracey, Acting Assistant Secretary for Information and Technology, Department of Veterans Affairs, and the Hon. John Dyer, Principal Deputy Commissioner, Social Security Administration.

Gentlemen, I am sure you have enjoyed the hearing so far this morning. As I say, we did not particularly mean to single you out, but we did because you do have areas that the GAO has made an assessment on. They will be making other assessments with regard to other agencies and departments in the future and I am confident that they will find the same kinds of problems. So we are not here to be overly critical of your particular agencies, but we are here to focus on what we plan on doing about it, the problems that we have. So we would appreciate any statements that you would care to make.

STATEMENT OF HAROLD F. GRACEY, JR.,[2] ACTING ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY, DEPARTMENT OF VETERANS AFFAIRS

Mr. GRACEY. Mr. Chairman, Members of the Committee, I am pleased to be here, in spite of what I have had to listen to this morning, because part of my job, like everybody's in government, is to take things that are not perfect and make them better.

You have my formal written statement, which I would ask to be included in the record.

Chairman THOMPSON. It will be made a part of the record.

Mr. GRACEY. To save time and to focus on where I am concentrating, I would only add that I share your concern about information systems security. I came to this current job only 3 months ago from being the Chief of Staff of the Department of Veterans Affairs for the previous 4½ years. This was the first issue that landed on my doorstep and the piece of it that I am most concerned about is that this is not new news to our Department. It is, however curiously, and perhaps it points to the issue of awareness, the first I have heard, in spite of having been at the right hand of the

[1] GAO Report entitled "Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk," appears in the Appendix on page 127.

[2] The prepared statement of Mr. Gracey appears in the Appendix on page 74.

Secretary and Deputy Secretary for 3 years, that we had a significant problem in the area of information system security.

The systems we operate at our Department contain much crucial and sensitive data on millions of our Nation's veterans. Safeguarding that information and protecting those systems is very important to the trust that veterans have in us and in the government. It is important to me, it is important to the Department at large, and we have acted quickly now on some of the specific issues the GAO has pointed out and our own Inspector General has pointed out in the course of their reviews. We are addressing those individual problems, solving those individual problems.

We have also acted to strengthen our planning, but I think I would agree with Mr. Dodaro from GAO, who said earlier that we have much work to do, first communicating among ourselves, to our employees, to our managers the criticality of this issue.

Second, not only completing policies and plans, but making the policies and plans real, turning them into action on which real changes are made, and then making sure that our protective actions work, monitoring not just whether people have followed the guidance, but whether the guidance was adequate in preventing the problem, making sure that our systems are safe and secure.

That is all I would offer now. I would be pleased to answer any of your questions.

Chairman THOMPSON. Thank you very much.

Mr. Dyer.

STATEMENT OF JOHN R. DYER,[1] PRINCIPAL DEPUTY COMMISSIONER, SOCIAL SECURITY ADMINISTRATION

Mr. DYER. Mr. Chairman, thank you, and I thank the Members of your Committee for inviting me here today to discuss the issues of computer security at the Social Security Administration.

I would like to begin by assuring this Committee and the American public that nothing is more important to our agency than to maintain the security of taxpayer information placed in our trust. In fact, after the creation of the Social Security program in 1935, the first regulation our agency issued dealt with non-disclosure of SSA record data. Today, this principle remains a cornerstone of everything we do.

We have taken actions to protect the information in our file from any wrongful use or unauthorized access by outside parties and it is important to note that SSA mainframe computers have never been successfully penetrated by outside parties. The agency's emphasis on system security is also demonstrated by the measures we have taken to prevent security breaches by our employees.

We pay benefits every month to almost 50 million Americans, and in order to do our work, as many as 60,000 of our 66,000 employees must have access on a need-to-know basis to computer records. This creates an inherent tension between the need of our workforce in being able to deliver the right benefit payment to the right person and the need to have the tightest possible systems security. When the agency learns an employee has abused his or her

[1] The prepared statement of Mr. Dyer appears in the Appendix on page 78.

systems privilege, steps are taken immediately to impose penalties as severe as termination of employment for the individual.

How do we ensure security in this work environment? First, SSA has a full-time staff devoted to systems security throughout the agency and SSA uses state-of-the-art software to restrict any user access to data except for its intended use. We are able to audit and monitor the actions individual employees take when using the system and we are able to investigate allegations of misuse. As part of our zero tolerance for fraud policy, the Commissioner issued a notice to all SSA employees this past June about administrative sanctions that will be taken against any employees who abuse his or her system privileges. Penalties are severe.

Further indication of our vigilance in security issues is that Social Security has a Chief Financial Officer who assures that all new systems have financial controls to maintain sound stewardship over the taxpayer monies entrusted to our care. Let me briefly review current systems security issues at Social Security.

As you know, Social Security has prepared a financial audit statement since 1987. In our 1997 statement, we received a clean audit opinion from our IG, through its contractor, for the fourth consecutive year. However, the 1997 contracting auditor, PricewaterhouseCoopers, also provided the agency with recommendations on how we could improve our systems safeguards and financial management controls.

We are in agreement with almost all the recommendations and over the past few months have worked closely with PricewaterhouseCoopers to determine how best to achieve the objectives of their recommendations. PricewaterhouseCoopers is now reviewing our progress and will report on this effort as part of the fiscal year 1998 audit of SSA's financial statements.

The changes being made as a result of the recommendations fall into four primary areas: One, improved controls to protect information; two, improvement in testing our plan for maintaining continuity of operations; three, improvement of our software application development and our control policies and procedures; and four, improved controls over separation of duties.

My written testimony includes detailed information about each of these recommendations and about the subsequent actions taken by SSA. In essence, over 60 percent of the PricewaterhouseCoopers recommendations have been implemented and the rest are being addressed expeditiously. Thus, the areas GAO cited earlier this morning are under control.

But I would like at this point to return to the broader concerns involved in the issue of computer security. By design, SSA has used a computer system architecture that relies almost exclusively on mainframe systems and centralized databases. With this architecture, we have been able to more tightly control computer security than those agencies that have to rely on local and distributive systems. However, the new technological environment requires that SSA now move away from mainframe environments to more distributive systems, and we need to carefully consider how to build security features in every step of the process.

We are supportive of independent audits of our financial statements and of detailed testing of agency systems. We believe it is

important to work with various oversight bodies to review what we are doing and identify any issues that need to be addressed. Only in this way can we be assured that SSA is doing the utmost to maintain the security of our computer systems and the data they contain.

Finally, let me repeat what I said at the outset. The Social Security Administration has no higher priority than being able to assure the American public that their personal records are secure. We also know that this is an ongoing obligation and that constant vigilance is required. I want to thank the Committee and you, Mr. Chairman, for holding this hearing and focusing on what we all view as a critical concern. I would be happy to answer any questions you may have.

Chairman THOMPSON. Thank you, Mr. Dyer.

As you know, in 1997, under the supervision of the GAO, the Social Security Administration Inspector General brought in a contractor to examine the Social Security computer security controls and to perform penetration testing on the agency's computer systems. In layman's terms, the point of the examination was to see whether the administration was adequately protecting itself from the risk of hackers breaking in from the outside and also engaging in computer fraud by employees from the inside.

The GAO discovered, as you know, shortcomings in both regards. Weak computer password practices which greatly diminish a crucial line of computer defense. Audit trail mechanisms that track browsing by Social Security employees and databases containing personal information on people were not properly set up or were being ignored by managers.

They found computer network control weaknesses that could result in accidental or intentional alteration of birth and death records, as well as unauthorized disclosure of personnel data and Social Security numbers, unprotected modems which permit remote access to Social Security Administration computers over phone lines, making it possible for unauthorized outsiders to enter Social Security Administration computer networks and modify, access, delete data, invent employees with computer access, deny access to legitimate employees and shut down computer systems in large portions of SSA's networks, various holes that allowed the friendly hacker contractors working under GAO's supervision to penetrate several SSA computer systems where they were in a position to view, alter, delete important data, and disrupt computer services by shutting down or reconfiguring computer networks.

As one example, hackers were able to take control of the SSA E-mail system. They could have shut it down, altered it, or have sent fake E-mails from any employees, including the SSA Commissioner.

GAO concluded these vulnerabilities expose SSA and its computer systems to external and internal intrusion, subject sensitive SSA information relating to Social Security numbers, earnings, disabilities, benefits to potential unauthorized access, modification, and/or disclosure, and increase the risk of waste, fraud, and abuse. Do you essentially agree or disagree with the GAO's findings here?

Mr. DYER. I agree with GAO that we need to do better. We wanted to have the outside auditor come in and look at our systems, be-

cause you constantly want to have someone telling you what may be wrong and where you may be vulnerable.

On the other hand, I think the way GAO has characterized this makes it sound as if things actually happened. A lot of what they are saying are potential things that could go wrong. Some of the areas where they have penetrated us were what I call our perimeter systems. But I do want to emphasize that the GAO and IG reviews done by people from outside SSA, came up with things that we were not aware and we had not seen in previous audits that had been done. We are jumping on these findings.

Chairman THOMPSON. Things did not happen because they were working for the government. They did not want to shut the system down or invent new people or things of that nature. But you do understand things could have happened if they had wanted it to.

Mr. DYER. Sure. There were potential things that could have happened and that is why we all want constantly to have outside people looking at you and working with you so you can see where your vulnerabilities are.

Chairman THOMPSON. You were not aware of previous reports, you said? What was that?

Mr. DYER. There were things that came up in this audit that had not been flagged for us in previous audits. That would be fair to say because this was, as Gene Dodaro said, a very systematic, broad kind of audit that had been done.

Chairman THOMPSON. Mr. Gracey, you said some of this was news to you, too. Similar problems were previously reported by your own IG. I do not know if that would have been in your line of authority at the time or not, but I do not think this is news to the top levels of the Veterans Administration.

Mr. GRACEY. That unique organizational-specific, system-specific weaknesses existed was not news to me. That we had major failings in our general planning and preparation for protecting our systems was news to me.

Chairman THOMPSON. You did not know that you had no security management program as such?

Mr. GRACEY. No, and I think, Mr. Chairman, that is one of those issues that reasonable people could differ on. As GAO said before us, we have elements of a program. Whether or not those elements add up to a program or not, I would not quibble, because, frankly, even if we had a program, I would not be happy with it because it is not doing what it is supposed to do. We have elements. We are missing other elements. We clearly have weaknesses. We are clearly concerned about that.

Chairman THOMPSON. GAO stated today that the VA had not established an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious intrusion activity. Has the VA now established an ongoing program to monitor and detect attacks on the system?

Mr. GRACEY. We have. We have begun the establishment of such a system. It exists in some places. It does not exist in others. I expressed, as I opened, one of the things in an organization as big as ours that is troublesome—we have 220,000 employees, more than 1,000 locations around the country—is that a plan is only as good as it is executed. So we need to be very sure that we put in

a monitoring system that not only monitors the implementation of the plan, but also monitors whether the plan accomplishes what it is supposed to accomplish—which is to prevent unauthorized access to our systems.

Chairman THOMPSON. Mr. Dyer, it sounds like much of the risk in the Social Security Administration is from current employees who are authorized to access SSA systems but have malicious intentions, and you heard the testimony that perhaps there are too many people with access. Do you agree with that, and can you tell me what controls the administration has in place to catch employee computer misconduct now?

Mr. DYER. I first want to say that I agree with the GAO that you always have the potential for internal vulnerability from your employees. On the flip side, when you look back over the data over the years and what the IG and others in investigation have found, there have been in our case very, very few employees who have misused our computer systems. We have basically 99.97 percent good employees. I want to start with that.

To secure SSA records from employee misconduct, we have done a lot of things. As I mentioned in my testimony, we toughened the penalties and made them very clear. We have reiterated the penalties in a more forceful way and we have the IG working with prosecutors to see if we can not get better enforcement.

Also, we knew that we needed more intelligence, so we have increased, as the IG mentioned to you, the size and focus of his staff and given him more resources and tools for him to do his job.

Because in many cases of employee fraud, you really cannot catch them before they do it, the question is how do you catch them after the fact? We have audit trails and we have moved to make them a little bit more automated and we have new systems that we are going to be developing for audit trails so we can utilize them faster.

Chairman THOMPSON. It sounds like those audit trails are so voluminous that it encourages people maybe not to use them as much as they should.

Mr. DYER. Yes, there are a lot of data in there, and right now you cannot manually take advantage of all the data you get out of the audit trails. What we try to do is figure out what things we should look for. Some things, we have automated. I do not want to get into details, but with regard to Social Security numbers we now have a way that we can automatically capture some of that.

The other thing we do is when we deal with our security officers around the country, we have told them what to look for, what kinds of profiles. We are now, with systems as the priority, moving to do a lot more automating so that you can go through the data fast, and catch trends; we can cover longitudinal distances and what not. So the equipment can get us the information faster.

Also, we are learning from the data. When the IG finds something or we get wind of something, we have an approach to address the problem. We figure out how to create a profile for that problem, which is what insurance companies do and other groups do when they are trying to defend themselves from these kinds of activities.

I think it is also important to get more prosecutions. You have got to deliver this message. The deterrent is that the employees

and others know that there is a chance they will get caught, in reasonably quick time, and that when they do get caught, the penalties are very severe.

Chairman THOMPSON. Like maybe even more than a $100 fine?

Mr. DYER. That is right. More than 4 months suspended sentence at home.

Chairman THOMPSON. Well, that has more to do with my other Committee, Judiciary, and these judges we approve that when they come and——

Mr. DYER. Any help you could give us there, we would appreciate.

Chairman THOMPSON [continuing]. All the statements that they make about what they are going to do and so forth before they get their lifetime appointment.

Let me ask you this, each of you. What interface have you had over the last year or so, or your department, with the OMB with regard to addressing this problem, if any?

Mr. GRACEY. This has been a point of discussion and concern at the Chief Information Officers Council, which I am new to, but it has come up on my screen, as I said, in the first several months of this job. In fact, I had a meeting just 2 weeks ago with the security champion, as he is referred to, for the Chief Information Officers Council, who is working to spread the best practices that Mr. Dodaro described, and others, around among the community of Federal departments and agencies.

So I would say it has had some attention. Clearly, there are other things that have been more urgent, the year 2000 among them, but it has received some focus. It has not received the amount of focus inside the VA that it needs and we are going to cure that.

Chairman THOMPSON. I am talking about specifically with regard to your discussions with OMB concerning this problem. Have you had any discussions or directives from OMB with regard to this specific problem?

Mr. GRACEY. I do not recall any directives, but there have been discussions, yes.

Chairman THOMPSON. With whom?

Mr. GRACEY. With Ed Deseve, who is the Deputy Director for Management, I believe, and——

Chairman THOMPSON. And who in your shop?

Mr. GRACEY. Myself.

Chairman THOMPSON. What was the nature of those discussions?

Mr. GRACEY. That, in fact, this was an issue of some high profile that we were all going to need to worry about, and then——

Chairman THOMPSON. Was it in the context of the Chief Financial Officers or Chief Information Officers Act requirements?

Mr. GRACEY. Yes, within the context of the Chief Information Officers Act and Council. And then again, I had a conversation with the designated champion—the Chief Information Officers Council works under the leadership of and in partnership with OMB. The fellow, I believe, is from the Department of Commerce who has taken on the lead role in security. He came to visit me and my staff with his staff and we discussed some of the issues. We have some

folks working with him to get best practices, get that spread across our department as well as others.

This is going to become an even bigger issue, Mr. Chairman, as we expand our systems to be new, more modern systems, as Mr. Dyer mentioned. It is an issue that we are all very much concerned about.

Chairman THOMPSON. Have there been any directives or guidelines that have come from OMB with regard to this matter——

Mr. GRACEY. Not that I am familiar with.

Chairman THOMPSON [continuing]. In addition to an expression of concern?

Mr. GRACEY. Not that I am familiar with, but I am new.

Chairman THOMPSON. Well, you would know about that if they were lying around over there somewhere, would you not?

Mr. GRACEY. I hope I would.

Chairman THOMPSON. Mr. Dyer, what about you?

Mr. DYER. We have had discussions with OMB when we got our audited financial statement. I talked to Ed Deseve, who is the focal point in OMB for this kind of thing. He heads up the management side. We have worked with his staff. We went through what the recommendations showed and what our concerns were.

Chairman THOMPSON. Well, you keep going back to that audit, and that is important, but that covers a lot of stuff that we are not dealing with here.

Mr. DYER. No, but I keep saying, a lot of what the GAO has been alluding to or the problems they have found were found by PricewaterhouseCoopers when they did the financial audit.

The second thing is that I have been on the CIO Council for a couple of years now and the CIO Council has moved to the front, next to Y2K, the whole question of security. But I will be very candid with you, Mr. Chairman, security has to be an agency initiative. OMB can send directives all over town. It can support us in dollars and cents, which we have received from OMB over the years and from the Congress. But each agency has to decide it is going to do it.

Where we find the CIO Council and these other groups useful is the exchange of information and knowing what is the latest information. The CIO Council sponsored a symposium recently. We sent some of our people to make sure we are up to speed, hearing what other agencies are going up against and learning, because you learn from other people's experience.

Chairman THOMPSON. Well, maybe I do not understand the nature of their job, then. I thought the "M" in OMB had to do with management.

Mr. DYER. Well, they focused in on the problems that we found and we have been working with them and the message I have gotten from them is "fix it." I am working on fixing the problems that were found.

Chairman THOMPSON. Well, to be continued. I think, if nothing else, we all have a better understanding of the nature of the problem. We are all trying to get to the same place. So let me encourage you to continue to do that, but also assure you that we will continue to be looking at this and next time we will have all been put on notice of these problems and we will be asking questions about

what is being done in order to make progress toward dealing with them.

I appreciate your being here today. Thank you very much.

Mr. GRACEY. Thank you.

Mr. DYER. Thank you.

Chairman THOMPSON. We are adjourned.

[Whereupon, at 11:50 a.m., the Committee was adjourned.]

APPENDIX

LETTER FROM MR. HUSE TO SENATOR THOMPSON

THE HON. FRED THOMPSON
Chairman, Committee on Governmental Affairs
U.S. Senate
Washington, DC 20510

DEAR MR. CHAIRMAN: Thank you for the opportunity to provide the Committee on Governmental Affairs with a formal statement, for the record, that conveys my views on the importance of the relationship between Inspectors General (IG) and agency heads and changes to the IG Act that are proposed in S. 2167.

I see the role of the Office of the Inspector General (OIG) within an agency as being constructive as well as instructive. I believe each OIG should ensure that its function exists as a valued part of the agency it serves. Too often, the model of an OIG's interactivity within an agency is (because of a misunderstanding of the concept of IG independence) one of confrontation and isolation. This type of interaction engenders an adversarial and sometimes hostile relationship between an IG and his/her agency. I am convinced that this is a distortion of the Congress' intent when it passed the IG Act of 1978.

It is critical for an IG to maintain independence and objectivity and yet foster a positive cooperative relationship with the head of his/her agency. IGs must balance their need for independence with an equal responsibility to become a valued partner in the agency they serve. This relationship should be built on a foundation of mutual respect. To attain this relationship, the IG must be perceived as fair-minded. As agents of positive change, IGs must ensure that their activities are above-board and that they do not hold the agency to a different set of standards than they hold themselves. This enhances an agency's trust in the OIG and makes the head of the agency more amendable to their recommendations. An IG whose reports and counsel are ignored or rejected has no utility.

Regarding the proposed changes to the IG Act, I believe the most important one is giving each IG a fixed term. Because an IG needs to sustain a relationship of respect and self-confident counsel with the head of an agency, they need legislated tenure over fixed terms of office. This legislative adjustment would ensure that IGs maintain their independence within an agency's organizational structure. IG tenure and fixed terms would also attenuate the tendency of some IGs to distance themselves from the leadership of their agencies.

If I can be of any further assistance regarding this matter, please call me or have your staff contact Stephanie J. Palmer, Acting Assistant Inspector General for External Affairs.

Sincerely,

JAMES G. HUSE, JR.
Acting Inspector General

SYSTEMS SECURITY WEAKNESSES

TESTIMONY BEFORE THE SENATE COMMITTEE ON GOVERNMENTAL AFFAIRS

September 23, 1998

JAMES G. HUSE, JR.
ACTING INSPECTOR GENERAL

Mr. Chairman and members of the Committee, thank you for inviting me to appear today to discuss system security weaknesses and employees who took advantage of these weaknesses to commit fraudulent activities at the Social Security Administration (SSA).

In response to a request from this Committee regarding the vulnerabilities of SSA systems, we have come to discuss the types of cases that have the highest priority; that is, employee fraud cases. When the SSA Office of the Inspector General (OIG) was established, the Commissioner of Social Security asked that employee integrity investigations be our paramount mission. System security is very important, and although we can have the best security in place, if employees are compromising system security, the system becomes flawed.

Identifying, investigating, and prosecuting SSA employees who inappropriately or criminally misuse their access to SSA electronic records systems to commit program fraud and other crimes is the number one priority of the SSA OIG. SSA components through our fraud referral process, inform OIG of suspicious behavior or allegations of suspicious behavior by employees for evaluation and consideration. This includes the results of periodic audits of employee system accesses that supervisors are required to conduct. Because of SSA OIG's cooperative relationship with SSA, we are able to deter employee fraud by seeking prosecution against employees who commit criminal violations and publicizing these prosecutions.

One of SSA OIG's major efforts in the detection of fraud is OPERATION CLEAN SLATE, which is designed to identify and prosecute employees who fraudulently manipulate SSA's electronic record systems to commit program fraud and other crimes. Under OPERATION CLEAN SLATE we have a number of initiatives designed to identify employees who abuse the Social Security data they have access to. We also exchange information with other Federal law enforcement agencies, such as the United States Secret Service, the Immigration and Naturalization Service, and numerous State and local law enforcement agencies, to vigorously investigate and prosecute career criminals who deal in Social Security fraud.

Today we will discuss some of the cases and projects that resulted from OPERATION CLEAN SLATE.

One of these projects, OPERATION PINCH, was initiated in late 1995, when SSA advised OIG of a possible corrupt employee in a New York Office. This fact was coupled with information received from the Citicorp Fraud Investigation Unit, Hagerstown, Maryland, who contacted SSA OIG in early 1996 to advise us of a major credit card fraud ring operating in the New York area. They informed us that stolen credit cards were being activated by contacting an "800" telephone number and supplying the card holder's name, SSN, and mother's maiden name. Citibank provided us with a list of 52 fraudulently activated credit card holder's SSNs and requested that SSA initiate data runs to determine if any SSA employees queried the same SSNs through the SSN data base on or about the activation date of the credit card holder's card. With full cooperation from SSA, a query of Social Security records found that employees had accessed the subjects records.

OPERATION PINCH was a criminal investigation in which a group of West African co-conspirators targeted the SSA data base for information needed to activate stolen credit cards for financial gain. These individuals obtained the SSNs associated with the stolen credit cards from various sources who had access to credit bureau records. They accomplished their goal by providing lists of SSNs to either SSA employees directly or indirectly through other associates. They elicited the SSA data for mothers' maiden names by offering bribes to the SSA employees. Many credit card companies require customers to contact a "800" telephone number to activate credit cards and require that SSNs and mothers' maiden names be provided as identification requirements. By using an audit trail software established by SSA to associate inquiries made of SSA computer system records by SSA employees, via a personal identification number, OIG and SSA were able to identify potential criminal violations. In addition, the investigation revealed that mother's maiden names and dates of birth were also being used by the West African co-conspirators to change the addresses of the true account holders and identity takeovers for illegal purposes; i.e., fraudulent loans, etc. No Social Security data of the actual account number holders were affected in any manner.

Through March 1996 to June 1996, the financial community continued to provide additional data to be run against the SSN files accessed by suspect employees. The data matches resulted in the identification of several employees. Through the interviews of these suspect employees, their admittances, and further investigation, additional employees, contract security guards at SSA facilities, and several West African and other co-conspirators were identified and prosecuted. Credit card fraud investigators from Citibank, Chase Manhattan Bank, Bank of America, and NOVUS provided additional information to us on stolen credit cards and their subsequent activation and the West African Task Force of the United States Secret Service supported our Agency's investigation.

This information resulted in the identification of several credit card fraud conspiracies in the New York area that included 12 SSA employees, 3 contract SSA Security Guards, and a New York City Human Resources Administration case investigator. Two employee investigations also took place in Milwaukee, Wisconsin, and Los Angeles, California. In addition, co-conspirators were also developed in Washington, D.C., Baltimore, Maryland, and Dallas, Texas. During the course of our investigation we determined that 20,000 names were furnished by SSA employees to the West African co-conspirators. According to financial institutions, fraud loss per activated stolen credit cards is estimated at $3,500. The credit card companies estimated the loss at $70,000,000. These dollar amounts reflect the total amount of fraud perpetrated by various criminals and should not be attributed to activities conducted by SSA employees alone. Throughout this investigation we have been able to identify that these 12 employees accessed thousands of SSN records and, based on the interviews of the employees, they received approximately $10 to $50 per SSN run.

Now I would like to specifically address seven investigations that were part of Project OPERATION PINCH in the New York Field Division:

1. Of the 52 SSNs provided by Citibank, 23 had SSN queries made by SSA employee **LESLIE ALVARADO** prior to the activation of the cardholders stolen credit card. **MS. ALVARADO** was a GS-8 Contact Representative in the Boro Hall District Office in Brooklyn, New York. During an interview with Special Agents from our office, **MS. ALVARADO** admitted to obtaining 30 Social Security account histories a day for a period of 2 years. She informed us that she provided the SSNs to a West African employee of the New York City Department of Human Resources Administration, Department of Social Services who used the information to activate stolen credit cards. She also obtained a second Social Security account number for the city employee, knowing that he already had a number issued to him.

MS. ALVARADO subsequently resigned from her position with the SSA and was arrested for Conspiracy to Commit Computer Fraud. **MS. ALVARADO** later pleaded guilty to two felony counts. The first count was for Conspiracy to Commit Unlawful Accessing of the Social Security Administration's data bases, and the second count was for Unlawful Issuance of a Second Social Security account number. She was sentenced to 5 years supervised probation and ordered to pay a $100 fine.

2. Another query of the SSN data base identified **YOLANDA MILFORD**, a GS-5 Claims Clerk in the North-Eastern Program Center in Jamaica, New York, who accessed the SSA system at an unusual high rate. The SSA records reflected that **MS. MILFORD**, who had minimal need to access the data base system, had conducted 655 record searches in a 6-month period. During an interview, **MS MILFORD** admitted selling 1,000 to 1,500 account records to co-conspirators for between $10 and $20 each.

MS. MILFORD resigned from her position with the SSA and was arrested July 15, 1996, for Conspiracy to Commit Credit Card Fraud and Conspiracy to Commit Computer Fraud. She pleaded guilty to one count of bribery on October 10, 1996. On March 14, 1997, **MS. MILFORD** was sentenced to 4 years probation and fined $2,000.

3. Based on the results of a local District Attorney search warrant, numerous Social Security records were obtained from a private New York residence. A review of these documents revealed that **CARLA AMEVOR**, a GS-8 SSA Contact Representative in the Jersey City, New Jersey, Teleservice Center, had accessed these accounts. During our interview, **MS. AMEVOR** admitted providing approximately 100 SSN records to a West African co-conspirator and receiving $15 per record, totaling $1,500 in illegal payments.

MS. AMEVOR resigned from her position with SSA and was arrested November 19, 1996, for Conspiracy to Commit Computer Fraud. **MS. AMEVOR** pleaded guilty on January 22, 1997 to Conspiracy to Engage in Unauthorized Use of a Government Computer. She was sentenced on April 30, 1997, to 2 years probation with the special condition to seek psychological counseling and fined $500.

4. Another query of the SSN data base identified **ERNEST MACASET**, a GS-4 Clerk Typist at the Flatbush District Office in Brooklyn, New York. During our interview, **MR. MACASET** advised us that he had been approached by the contract SSA Security Guard at his office to sell Social Security record information for $50 to $100 per record. Between November 1995 and April 1996, **MR. MACASET** sold SSN records to the guard. He further advised us that since the guard only paid him $40 per record, he discontinued selling SSA records. He further identified a West African co-conspirator as an individual to whom he sold SSA records for $50 per record from April 1996 through the end of July 1996. **MR. MACASET** was immediately terminated from SSA employment and was later arrested for bribery. On March 6, 1997, he entered a guilty plea for one count of Disclosure of Confidential Information. On July 3, 1997, he was sentenced to 3 years probation, fined $8,343, and ordered to pay restitution in the amount of $20,239 to financial institutions.

5. Through our investigations of employees at the Flatbush District Office of SSA, **EUGENE RYBALSKY**, a Stay-in-School Clerk Typist (SIS) (GS-4), was identified as accessing SSA records and furnishing them to the office Security Guard. During the interview, **MR. RYBALSKY** refused to cooperate.

MR. RYBALSKY was immediately terminated from SSA employment and was later arrested on November 19, 1996, for violation of bribery. On January 31, 1997, **MR. RYBALSKY** pleaded guilty to one count of Disclosure of Confidential Information. He was sentenced on May 2, 1997, to 3 years probation, 200 hours community service, and fined $25.

6. Through our investigations of employees at the Flatbush District Office, **MICHAEL WATKINS**, SIS Clerk Typist (GS-4), was identified as accessing SSN records and selling them to the office Security Guard. During our interview, **MR. WATKINS** admitted to providing SSA records to the office Security Guard. A review of SSN records revealed that **MR. WATKINS** conducted approximately 2,400 SSN searches in 18 months. **MR. WATKINS** was immediately terminated from SSA employment and later arrested in November 19, 1996, for bribery, more specifically, for his involvement in the sale of SSN records. On January 28, 1997, he pleaded guilty to 1 count of Disclosure of Confidential Information. On April 29, 1997, he was sentenced to 2½ years probation and 6 months home confinement.

7. A further review of SSN data base records in comparison to stolen credit card activation identified **LENA MORTON**, a GS-5 Claims Clerk in the Bronx River Parkway Branch Office, as accessing data base records. During our interview, **MS. MORTON** admitted to selling Social Security account records to the former Security Guard at her office for $15 per record.

MS. MORTON was terminated from SSA employment and was later arrested on September 19, 1996, for violation of Conspiracy to Commit Computer Fraud. On March 6, 1997, she pleaded guilty to one count of bribery. She was sentenced on July 7, 1997, to 3 years of supervised probation, assessed a $100 fine, and mandated to receive drug counseling.

Now I would like to discuss several additional significant employee cases that we have investigated that have resulted in prosecution.

1. On July 10, 1995, the SSA's Regional Security Office in San Diego, California, notified the recently established SSA OIG of allegations made by a private citizen that **WILLIAM JOSEPH YUST (Case No. L-95-01454-6)** had charged two individuals $100 each to waive the overpayments debited against their Social Security accounts. The SSA OIG opened an investigation and 4 months later learned from SSA management that **MR. YUST's** wife was reportedly threatening to advise the police that he was also selling Social Security cards.

A subsequent investigation by SSA OIG investigators revealed that **MR. YUST** illegally processed approximately 160 original or duplicate Social Security cards for approximately 133 individuals who were not entitled to have them. He admitted selling the Social Security numbers and cards for $200 each and using the proceeds to purchase drugs. **MR. YUST** explained that he was able to thwart detection of his unauthorized activity by altering the office code associated with each of his entries in the computer system. By changing his assigned office code to reflect the codes of various offices throughout the Nation, he reduced the likelihood that periodic security reviews would detect any unusual patterns of activity.

On May 5, 1997, **MR. YUST** pleaded guilty to one felony count of accepting a bribe and one felony count of processing and causing to be issued unauthorized Social Security numbers and cards. He was sentenced on August 4, 1997, to serve 3 years of supervised probation, to complete 50 hours of community service, and to pay a special penalty of $100. **MR. YUST's** employment was terminated on May 24, 1997, after a lengthy period of administrative leave.

2. The following case was initiated in 1997 by SSA OIG based on a referral from an outside law enforcement agency. This information was developed while debriefing a subject in a narcotics investigation. The subject provided information, which led to the identification of SSA employee **KATHLEEN DAIGRE (Case No. C-97-00124-D)** who was running a scheme to defraud SSA. A preliminary review of SSA records revealed **MS. DAIGRE** was employed as a GS-9 Benefit Authorizer at the SSA Payment Center in Kansas City, Missouri. In the capacity of Benefit Authorizer, **MS. DAIGRE** authorized SSA checks to be written and mailed to persons entitled to Social Security benefits.

Based on this information, SSA OIG requested that the SSA Security and Integrity Team perform a review of the SSNs that **MS. DAIGRE** had accessed as a part of employment. The review revealed that **MS. DAIGRE** had accessed and changed Social Security records pertaining to herself and family members. The Security and Integrity Service review determined that as a result

of the changes **MS. DAIGRE** had made to the Social Security records, unauthorized checks were issued from October 2, 1995 through November 2, 1996, to ten deceased beneficiaries and two living beneficiaries. **MS. DAIGRE** had changed the addresses of these beneficiaries in the Social Security records to reflect her address or her friends' addresses. In order to make the checks look legitimate, **MS. DAIGRE** used one of her former married names, her maiden name, or some variation thereof. Through interviews conducted by SSA OIG Special Agents, it was also established **MS. DAIGRE** had conspired with **MS. JUDITH METCALF**, a GS-9 Benefit Authorizer in the same Payment Center, to issue SSA checks to herself, her husband, her son, and a friend. The amount of the fraudulent checks issued by **MS. DAIGRE** and **MS. METCALF** totaled $174,312.30.

MS. DAIGRE and **MS. METCALF** were charged with Theft of Government Funds and Property. Both resigned their positions with SSA and entered into plea agreements for these charges with the stipulation that they confess to their wrongdoings and make restitution. **MS. DAIGRE** was ordered to serve 15 months in prison, 3 years probation, and pay restitution to SSA in the amount of $174,312.30. **MS. METCALF** was ordered to serve 5 years probation and pay restitution to SSA in the amount of $20,933.10.

3. In November 1993, a Chicago bank referred a case to OIG regarding suspicious account activity held by **ALBERT IRWIN (Case No. 5-93-01021-6)**, a GS-9 Benefit Authorizer at the Social Security Great Lakes Program Service Center. As a result of this referral, the SSA Great Lakes Program Service Center Integrity Staff conducted a review of **MR. IRWIN's** computer traffic and confirmed suspicious activity. In mid-1995, SSA OIG Special Agents interviewed **MR. IRWIN** who signed a written statement confessing to SSA fraud. Approximately 2 weeks later he resigned from his position with SSA.

The investigation disclosed that **MR. IRWIN** generated "one-check-only payments" to fictitious individuals by entering false data into the records of existing beneficiary accounts. By way of explanation, a "one-check-only payment" is a one-time, retroactive payment that can be sent to any person, account or address. For example, a survivor could receive an underpayment on a number holder's account. **MR. IRWIN** had a total of $84,463 directly deposited through such false entries to his personal account a the Chicago bank. He withdrew the money from his account and spent it for personal use.

In October 1996, **MR. IRWIN** pleaded guilty to one count of Wire Fraud in Federal District Court in Illinois and was sentenced to 1-year incarceration and restitution of $7,200.

4. The SSA OIG received an allegation that an SSA employee had improperly and maliciously changed the record (within the SSA data base) of an acquaintance. The fraud was initially detected when the victim applied for a bank loan. Through queries made by the bank, it was discovered that records pertaining to the victim reflected she was deceased. The victim personally called in the complaint.

The allegation identified **JORGE A. YONG (Case No. F-97-00323-C)**, a GS-11 Claims Representative at the Belle Glade, Florida District Office, as the subject. Allegedly, **MR. YONG** made an entry into the Social Security number record of the victim to indicate she was deceased. The victim is living in Naples, Florida.

The SSA OIG initiated an investigation and interviewed the complainant, the suspect, and employees of the Belle Glade, Florida District Office. The electronic logs for the SSA computer system were reviewed to develop a history of the entries made to the victim's account. That review found that another employee of the Belle Glade, Florida District Office had entered the date of death on the victim's record. Although that employee denied any wrongdoing, she recalled occasions she had left her SSA computer terminal unattended and returned to find other coworkers using it.

We found that the victim and **MR. YONG** were acquainted via Internet communications. The two had a disagreement, which precipitated **MR. YONG's** ban from an Internet chatroom they both frequented. Another Internet party informed the victim that **MR. YONG** had mentioned he had the ability to have the victim's SSN reflect that she was deceased.

MR. YONG was interviewed and admitted he had queried the Social Security data base concerning the victim. He also admitted that he used a coworker's terminal to make the date of death input into the victim's record. He confessed that he made these queries and inputs because of a personal conflict he had with the victim. **MR. YONG** subsequently resigned from employment with SSA.

Pursuant to an appearance before the U.S. District Court in Ft. Lauderdale, Florida, **MR. YONG** pleaded guilty to one count of falsifying the personal data filed and deposited with an agency of the United States. He was sentenced to 1-year probation, ordered to pay restitution in the amount of $700 to the victim, and pay a special assessment of $100 to the court. Additionally, he is expected to maintain a full-time job and refrain from Internet access during his probation period.

5. The SSA OIG received information alleging that Nationwide Electronic Tracking, Inc., of Tampa, Florida, was selling confidential Government information, including Detailed Earnings Queries unlawfully obtained from SSA and National Crime Information Center (NCIC) criminal histories unlawfully obtained from the Department of Justice (DOJ). An 18-month undercover investigation ensued which substantiated the allegation and resulted in the conviction of 21 individuals including 5 SSA employees, 1 SSA Government contractor, 2 law enforcement officials, and 1 Army Criminal Investigations Division Officer.

This case involved cooperating witnesses who bought and sold non-public information such as SSA records (Detailed Earnings Queries and SSN Queries) and DOJ - NCIC criminal histories. The investigation traced a nationwide network of information brokers and their sources. Even though this investigation dealt primarily with the theft of protected United States Government

information, it also showed how information brokers gathered protected information by "pre-texting" or "gagging." These practices involve tricking an individual via a telephone call, into providing information unwittingly; a violation of Fraud by Wire.

DONALD L. WRIGHT (Case No. 4-90-00327-6), a GS-7 Teleservice Center Representative at the Ft. Lauderdale Teleservice Center, had access to SSA's computer network. Our investigation substantiated that **MR. WRIGHT** had accepted bribes from information brokers in exchange for conducting unauthorized inquiries of Social Security records. **MR. WRIGHT** reportedly received approximately $3,000 for SSA information. He resigned from SSA after being interviewed by SSA OIG Special Agents.

For his role in the unauthorized access and sale of Government information, **MR. WRIGHT** was indicted and charged with a violation of Conspiracy. He eventually pleaded guilty to conspiracy and was sentenced to 2 months incarceration, 4 months of home detention with electronic monitoring, 2½ years probation, and a special assessment of $50.

The other subjects of this investigation were also convicted of various felony statutes including bribery, unauthorized disclosure of tax return information, theft of Government property, and conspiracy.

6. In March 1995, the following case was referred to OIG from the SSA Regional Security Staff in New Jersey, who had been contacted by a small New Jersey Bank regarding suspicious activity. The bank reported that a number of SSA electronic fund transfers (EFTs) in the amount of $2,999 each had been deposited into one of their customer's accounts. The EFTs were in different names and SSNs.

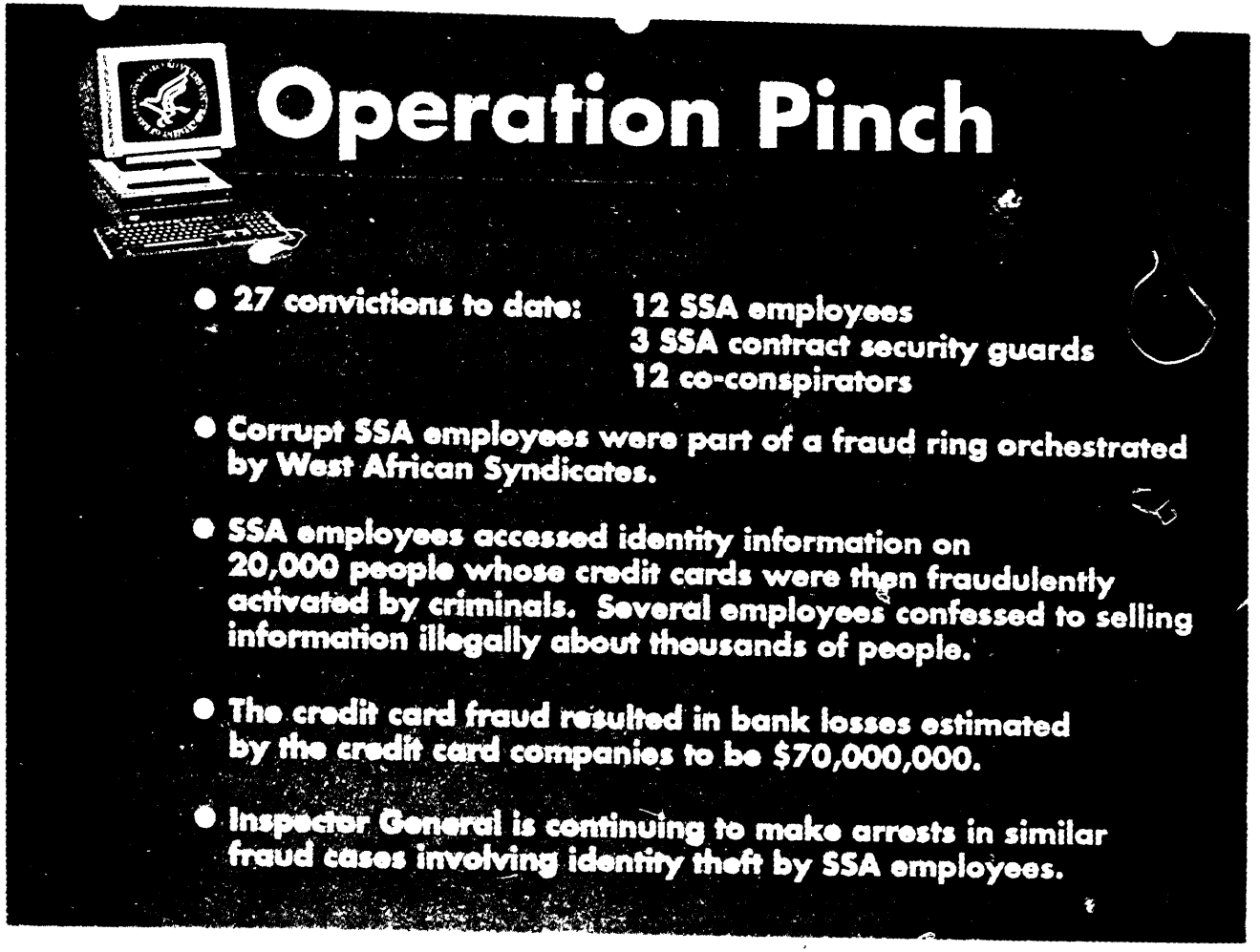
On March 24, 1995, the SSA OIG interviewed the account holder, who was not an SSA employee. The subject denied knowing how or why SSA funds had been sent to his savings account; however, he did admit to withdrawing and using the money in the account.

On March 28, 1995, SSA OIG, working with the SSA Northeastern Program Service Center (NEPSC) Security and Integrity Staff, determined that **RONALD SNODDY (Case No. 2-95-00300-6)**, a GS-9 Benefit Authorizer at the NEPSC, was involved in a scheme to defraud SSA. The investigation disclosed that, in his capacity as a Benefit Authorizer for SSA, **MR. SNODDY** authorized wire transfers of SSA funds to bank accounts held by himself and others who were not entitled to receive such funds. From March 1994 through March 1995, **MR. SNODDY** transferred approximately $328,731 in this manner.

The investigation led to the identification and prosecution of additional account holders, who were not SSA employees, who received SSA funds from **MR. SNODDY** through New Jersey and New York banks.

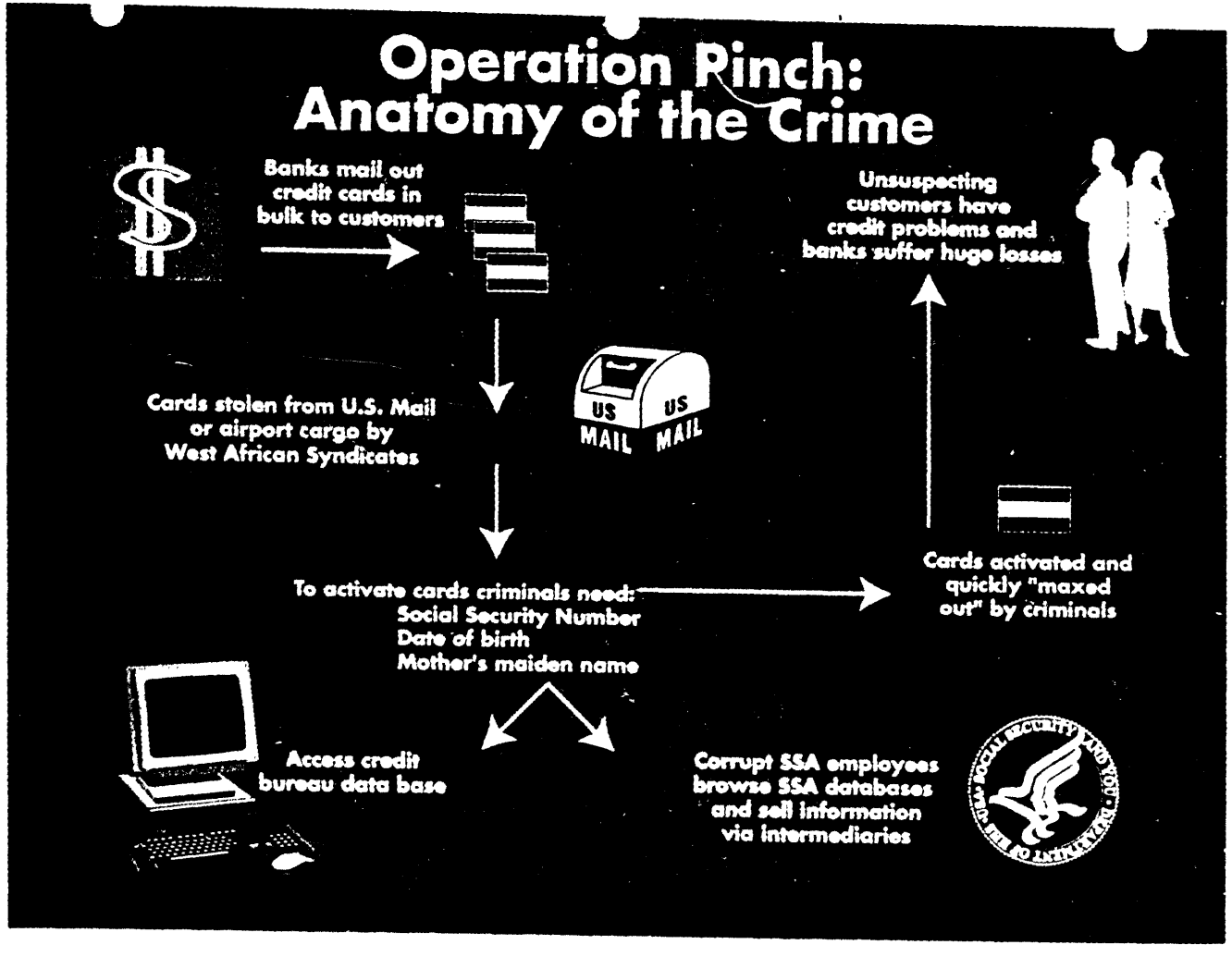
On April 6, 1995, **MR. SNODDY** was arrested by SSA OIG Special Agents on charges involving Wire Fraud and Money Laundering. On June 5, 1995, **MR. SNODDY** resigned his position at SSA. On September 28, 1995, **MR. SNODDY** pleaded guilty in U.S. District Court, Newark, New Jersey, to an Information charging him with Wire Fraud and Aiding and Abetting in Wire Fraud. On July 12, 1996, he was sentenced to 4 months imprisonment, 4 months home confinement, 3 years supervised release, restitution of $50,000, and a special assessment of $50. The Court waived the fine, however, due to the inability of the defendant to pay.

Employee fraud cases represent the smallest number of cases we investigate; however, employee fraud is the most serious matter that we must deal with effectively. We believe publicizing the cases we investigate and successfully prosecute is an effective deterrent against future employee fraud. OIG publicizes fraud cases by distributing fact sheets to SSA Regional Public Affairs Officers and SSA headquarters personnel. The Regional Public Affairs Officers prepare press releases and work with the local field office managers to get media coverage and to issue the press releases. We also transmit the findings to SSA Headquarters for distribution to SSA employees via SSA publications. In this way, prosecutions are made public and all SSA employees are made aware of the fact that employee misconduct will not be tolerated. Increasing OIG resources and recent access into SSA systems, will increase our abilities to identify and monitor suspicious activity and vulnerable areas. We are dedicated to eliminating employee fraud and misconduct at SSA. I wish to thank the Committee again for focusing on this important and serious issue and would be pleased to answer any questions you may have at this time.



Operation Pinch: Overview

- Massive credit card fraud and theft orchestrated by West African crime syndicates.
- Criminals stole thousands of credit cards mailed out to unsuspecting bank customers.
- Credit cards could be activated, via 1-800 phone lines, using card holders social security numbers, date of birth, and mother's maiden name as security prompts.
- Criminals enlisted corrupt Social Security Administration employees to obtain information needed to activate stolen credit cards.


Operation Pinch:
Anatomy of the Crime
Banks mail out credit cards in bulk to customers
Unsuspecting customers have credit problems and banks suffer huge losses
Cards stolen from U.S. Mail or airport cargo by West African Syndicates
US MAIL
US MAIL
To activate cards criminals need:
Social Security Number
Date of birth
Mother's maiden name
Cards activated and quickly "maxed out" by criminals
Access credit bureau data base
Corrupt SSA employees browse SSA databases and sell information via intermediaries

Recent Cases Involving "Insider" Computer Security Breaches By SSA Employees

- Sale of identity information to credit card fraud rings – Operation Pinch
- Fraudulent wire transfers of SSA benefit checks
- Sale of altered identity information to illegal immigrants involved in drug ring
- Sale of identity information to nationwide ring of private investigators and information brokers
- Alteration of SSA records to harass individuals

Social Security Cards for Sale

- SSA Teleservice Representative employee in San Diego Field Office created and sold approximately 160 Social Security cards and numbers for $200 each.
- Cards provided to members of drug ring who used them to provide identities for illegal immigrants.
- Employee manipulated Social Security computer systems to alter his office code to avoid detection by security reviews.

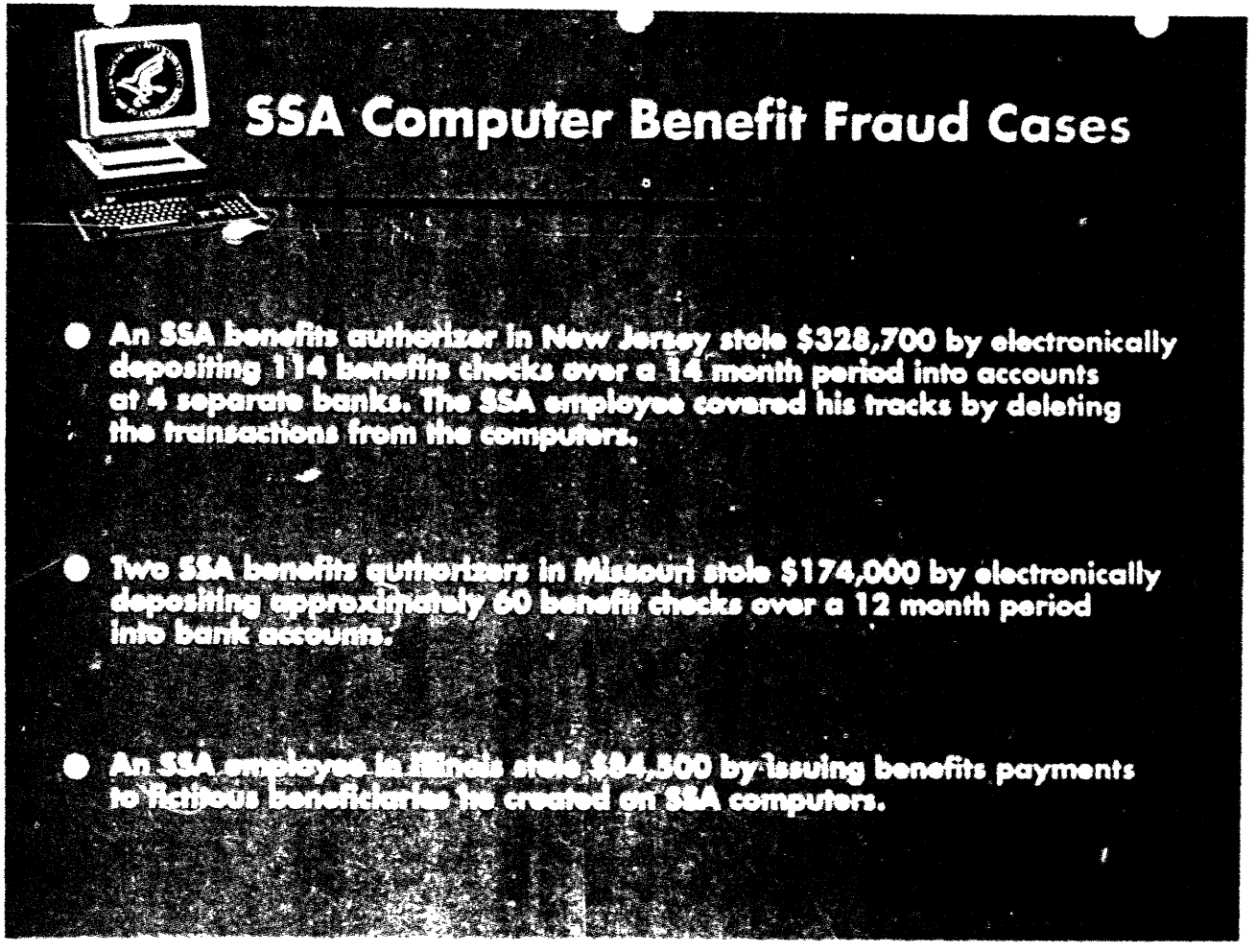
Illegal Sale of Identity Information to Information Brokers

- IG Investigation uncovered nationwide ring of information brokers who sold confidential information on individuals to private investigators, law firms, insurance companies, etc.
- 23 convictions, including five SSA employees from NY, NJ, IL, AZ, and FL.
- The five SSA employees sold confidential information obtained through unauthorized queries of SSA computer data, including SSN, dates of birth, and detailed wage and earnings information.
- SSA security measures did not identify or prevent unauthorized access by SSA employees.

Virtual Murder

- SSA Claims Representative from Florida District Office entered death notice into official SSA database record for an individual with whom he had a disagreement in an Internet chatroom discussion.

- Victim discovered her death notice while attempting to open bank account when bank officials indicated she was "dead", according to credit reports.


SSA Computer Benefit Fraud Cases
• An SSA benefits authorizer in New Jersey stole $328,700 by electronically depositing 114 benefits checks over a 14 month period into accounts at 4 separate banks. The SSA employee covered his tracks by deleting the transactions from the computers.
• Two SSA benefits authorizers in Missouri stole $174,000 by electronically depositing approximately 60 benefit checks over a 12 month period into bank accounts.
• An SSA employee in Illinois stole $84,500 by issuing benefits payments to fictitious beneficiaries he created on SSA computers.

United States General Accounting Office

GAO

Testimony

Before the Committee on Governmental Affairs, U.S. Senate

For Release on Delivery
Expected at
10 a.m.
Wednesday,
September 23, 1998

INFORMATION SECURITY

Strengthened Management Needed to Protect Critical Federal Operations and Assets

Statement of Gene L. Dodaro
Assistant Comptroller General
Accounting and Information Management Division

Mr. Chairman and Members of the Committee:

I am pleased to have this opportunity to provide an assessment of the current state of information security in federal government. Our most recent report, done at the request of this Committee, delineates the serious information security weaknesses placing critical operations and assets at risk and outlines actions needed to further improve security practices across government. The two agencies that you asked us to focus on today--the Department of Veterans Affairs and the Social Security Administration--illustrate the types of risk facing individual departments and agencies as well as actions required to strengthen security management. Recent efforts by these organizations and others throughout government are encouraging because they signify increasing attention to information security concerns, but, as we will discuss today, additional measures are necessary for the federal government to develop and maintain a truly effective security management program.

INFORMATION SECURITY IS DRAWING INCREASED ATTENTION

We last provided you an overview of federal information security in September 1996. At that time, serious security weaknesses had been identified at 10 of the largest 15 federal agencies, and we concluded that poor information security was a widespread federal problem.[1] We recommended that the Office of Management and Budget (OMB) play a more active role in overseeing agency practices, in part through its role as chair of the then newly established Chief Information Officers (CIO) Council. Subsequently, in February 1997, as more audit evidence became available, we designated information security as a new governmentwide high-risk area in a series of reports to the Congress.[2]

During 1996 and 1997, federal information security also was addressed by the President's Commission on Critical Infrastructure Protection, which had been established to investigate our nation's vulnerability to both "cyber" and physical threats. In its October 1997 report, Critical Foundations: Protecting America's Infrastructures, the Commission described the potentially devastating implications of poor information security from a national perspective. The report also recognized that the federal government must "lead by example," and included recommendations for improving government systems security. This report eventually led to issuance of Presidential Decision Directive 63 in May 1998,

---

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

[2]High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

which I will discuss in conjunction with other governmentwide security improvement efforts later in my testimony.

POTENTIAL RISKS ARE INCREASING

As hearings by this Committee have emphasized, risks to the security of our government's computer systems are significant, and they are growing. The dramatic increase in computer interconnectivity and the popularity of the Internet, while facilitating access to information, are factors that also make it easier for individuals and groups with malicious intentions to intrude into inadequately protected systems and use such access to obtain sensitive information, commit fraud, or disrupt operations. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are readily available.

Attacks on and misuse of federal computer and telecommunication resources are of increasing concern because these resources are virtually indispensable for carrying out critical operations and protecting sensitive data and assets. For example,

- weaknesses at the Department of the Treasury place over a trillion dollars of annual federal receipts and payments at risk of fraud and large amounts of sensitive taxpayer data at risk of inappropriate disclosure;

- weaknesses at the Health Care Financing Administration place billions of dollars of claim payments at risk of fraud and sensitive medical information at risk of disclosure; and

- weaknesses at the Department of Defense affect operations such as mobilizing reservists, paying soldiers, and managing supplies. Moreover, Defense's warfighting capability is dependent on computer-based telecommunications networks and information systems.

These and other examples of risks to federal operations and assets are detailed in our report Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92), which the Committee is releasing today. Although it is not possible to eliminate these risks, understanding them and implementing an appropriate level of effective controls can reduce the risks significantly. Conversely, an environment of widespread control weaknesses may invite attacks that would otherwise be discouraged.

SERIOUS WEAKNESSES CONTINUE
TO BE IDENTIFIED

As the importance of computer security has increased, so have the rigor and frequency of federal audits in this area. During the last 2 years, we and the agency inspectors general

(IGs) have evaluated computer-based controls on a wide variety of financial and nonfinancial systems supporting critical federal programs and operations. Many of these audits are now done annually. This growing body of audit evidence is providing a more complete and detailed picture of federal information security than was previously available.

The most recent set of audit results that we evaluated–those published since March 1996–describe significant information security weakness in each of the 24 federal agencies[3] covered by our analysis. These weaknesses cover a variety of areas, which we have grouped into six categories of general control weaknesses.

Access Control Weaknesses

The most widely reported weakness was poor control over access to sensitive data and systems. This area of control was evaluated at 23 of the 24 agencies, and weaknesses were identified at each of the 23. Access control weaknesses make systems vulnerable to damage and misuse by allowing individuals and groups to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities), thereby protecting them against unauthorized modification, loss, and disclosure.

Access controls include physical protections, such as gates and guards, as well as logical controls, which are controls built into software that (1) require users to authenticate themselves through the use of secret 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 today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to potentially devastating attacks from remote locations all over the world by individuals with minimal computer and telecommunications resources and expertise. Common types of access control weaknesses included

- overly broad access privileges inappropriately provided to very large groups of users;
- access that was not appropriately authorized and documented;
- multiple users sharing the same accounts and passwords, making it impossible to trace specific transactions or modifications to an individual;

[3]These agencies accounted for 99 percent of reported federal net outlays in fiscal year 1997.

- inadequate monitoring of user activity to deter and identify inappropriate actions, investigate suspicious activity, and penalize perpetrators;

- improperly implemented access controls, resulting in unintended access or gaps in access control coverage; and

- access that was not promptly terminated or adjusted when users either left an agency or when their responsibilities no longer required them to have access to certain files.

Service Continuity Weaknesses

The second most widely reported type of weakness pertained to service continuity. Service continuity controls ensure that, when unexpected events occur, critical operations continue without undue interruption and critical and sensitive data are protected. In addition to protecting against natural disasters and accidental disruptions, such controls also protect against the growing threat of "cyber-terrorism," where individuals or groups with malicious intent may attack an agency's systems in order to severely disrupt critical operations. 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. To determine whether recovery plans will work as intended, they should be tested periodically in disaster simulation exercises.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to accomplish its mission. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information.

Service continuity controls were evaluated for 20 of the agencies included in our analysis, and weaknesses were reported for all of these agencies. Common weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur.

- Disaster recovery plans were not fully tested to identify their weaknesses. One agency's plan was based on an assumption that key personnel could be contacted within 10 minutes of the emergency, an assumption that had not been tested.

Entitywide Program Planning and Management Weaknesses

The third most common type of weakness involved inadequate 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.

Weaknesses were reported for all 17 of the agencies for which this area of control was evaluated. Many of these agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on.

Segregation of Duties Weaknesses

The fourth most commonly reported type of weakness was inadequate 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.

Segregation of duties is an important internal control concept that applies to both computerized and manual processes.[4] However, it is especially important in computerized environments, since an individual with overly broad access privileges can initiate and execute inappropriate actions, such as software changes or fraudulent transactions, more quickly and with greater impact than is generally possible in a non-automated environment. Although segregation of duties alone will not ensure that only authorized activities occur, inadequate segregation of duties increases the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a combination of physical and logical access controls and by effective supervisory review.

---

[4]Title 2, "Accounting," Appendix II, "Standards for Internal Controls in the Federal Government", GAO Policy and Procedures Manual for Guidance of Federal Agencies.

Segregation of duties was evaluated at 17 of the 24 agencies. Weaknesses were identified at 16 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a wide variety of duties, thus enabling them to independently modify, circumvent, and disable system security features. For example, at one agency, all users of the financial management system could independently perform all of the steps needed to initiate and complete a payment–obligate funds, record vouchers for payment, and record checks for payment–making it relatively easy to make a fraudulent payment.

Application Software Development and Change Control Weaknesses

The fifth most commonly reported type of weakness pertained to software development and change controls. Such controls prevent unauthorized software programs or modifications to programs from being implemented. Key aspects are ensuring that (1) software changes are properly authorized by the managers responsible for the agency program or operations that the application supports, (2) new and modified software programs are tested and approved prior to their implementation, and (3) approved software programs are maintained in carefully controlled libraries to protect them from unauthorized changes and ensure that different versions are not misidentified.

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

Weaknesses in software program change controls were identified for 14 of the 18 agencies where such controls were evaluated. The most common type of weakness in this area was undisciplined testing procedures that did not ensure that implemented software operated as intended. In addition, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of locally-developed unauthorized software programs was prevented or detected.

System Software Control Weaknesses

The sixth area pertained to operating system software controls. System software controls limit and monitor access to the powerful programs and sensitive files associated with the computer systems operation. Generally, one set of system software is used to support and control a variety of applications that may run on the same computer hardware. System software helps control and coordinate the input, processing, output, and data storage associated with all of the applications that run on the system. Some system software can change data and programs without leaving an audit trail or can be used to

modify or delete audit trails. Examples of system software include the operating system, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

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

A common type of system software control weakness reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a wide variety of ways. For example, at one facility, 88 individuals had the ability to implement programs not controlled by the security software, and 103 had the ability to access an unencrypted security file containing passwords for authorized users.

Significant system software control weaknesses were reported at 9 of the 24 agencies. In the remaining 15 agencies, this area of control had not been fully evaluated. We are working with the IGs to ensure that it receives adequate coverage in future evaluations.

I would, now, like to describe in greater detail weaknesses at the two agencies that you have chosen to feature today: the Department of Veterans Affairs and the Social Security Administration.

WEAKNESSES AT THE DEPARTMENT OF VETERANS AFFAIRS

The Department of Veterans Affairs (VA) relies on a vast array of computer systems and telecommunications networks to support its operations and store the sensitive information the department collects in carrying out its mission. In a report released today, we identify general computer control weaknesses that place critical VA operations, such as financial management, health care delivery, benefit payments, life insurance services, and home mortgage loan guarantees at risk of misuse and disruption.[5] In

[5]VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical records and benefit payments, is vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction–possibly occurring without detection.

VA operates the largest health care delivery system in the United States and guarantees loans on about 20 percent of the homes in the country. In fiscal year 1997, VA spent over $17 billion on medical care and processed over 40 million benefit payments totaling over $20 billion. The department also provided insurance protection through more than 2.5 million policies that represented about $24 billion in coverage at the end of fiscal year 1997. In addition, the VA systems support the department's centralized accounting and payroll functions. In fiscal year 1997, VA's payroll was almost $11 billion, and the centralized accounting system generated over $7 billion in additional payments.

In our report, we note significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit the access of authorized users or effectively manage user identifications (IDs) and passwords.

- At one facility, the security software was implemented in a manner that provided all of the more than 13,000 users with the ability to access and change sensitive data files, read system audit information, and execute powerful system utilities. Such broad access authority increased the risk that users could circumvent the security software to alter payroll and other payment transactions. This weakness could also provide users the opportunity to access and disclose sensitive information on veteran medical records, such as diagnoses, procedures performed, inpatient admission and discharge data, or the purpose of outpatient visits, and home mortgage loans, including the purpose, loan balance, default status, foreclosure status, and amount delinquent.

- At two facilities, we found that system programmers had access to both system software and financial data. This type of access could allow the programmers to make unauthorized changes to benefit payment information without being detected.

- At four of the five facilities we visited, we identified user ID and password management control weaknesses that increased the risk of passwords being compromised to gain unauthorized access. For example, IDs for terminated or transferred employees were not being disabled, many passwords were common words that could be easily guessed, numerous staff were sharing passwords, and some user accounts did not have passwords These types of weaknesses make the financial transaction data and personal information on veteran medical records and benefits stored on these systems vulnerable to misuse, improper disclosure, and destruction. We demonstrated these vulnerabilities by gaining unauthorized access to VA systems and obtaining information that could have been used to develop a strategy to alter or disclose sensitive patient information.

We also found that the department had not adequately protected its systems from unauthorized access from remote locations or through the VA network. The risks created by these issues are serious because, in VA's interconnected environment, the failure to control access to any system connected to the network also exposes other systems and applications on the network.

- While simulating an outside hacker, we gained unauthorized access to the VA network. Having obtained this access, we were able to identify other systems on the network, which makes it much easier for outsiders with no knowledge of VA's operations or infrastructure to penetrate the department's computer resources. We used this information to access the log-on screen of another computer that contained financial and payroll data, veteran loan information, and sensitive information on veteran medical records for both inpatient and outpatient treatment. Such access to the VA network, when coupled with VA's ineffective user ID and password management controls and available "hacker" tools, creates a significant risk that outside hackers could gain unauthorized access to this information.

- At two facilities, we were able to demonstrate that network controls did not prevent unauthorized users with access to VA facilities or authorized users with malicious intent from gaining improper access to VA systems. We were able to gain access to both mainframe and network systems that could have allowed us to improperly modify payments related to VA's loan guaranty program and alter sensitive veteran compensation, pension, and life insurance benefit information. We were also in a position to read and modify sensitive data.

The risks created by these access control problems were also heightened significantly because VA was not adequately monitoring its systems for unusual or suspicious access activities. In addition, the department was not providing adequate physical security for its computer facilities, assigning duties in such a way as to properly segregate functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to ensure that the department could maintain or regain critical functions in emergencies.

Many similar access and other general computer control weaknesses had been reported in previous years, indicating that VA's past actions have not been effective on a departmentwide basis. Weaknesses associated with restricting access to sensitive data and programs and monitoring access activity have been consistently reported in IG and other internal reports.

A primary reason for VA's continuing general computer control problems is that the department does not have a comprehensive computer security planning and management program in place to ensure that effective controls are established and maintained and that computer security receives adequate attention. An effective program would include

guidance and procedures for assessing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. However, the VA had not clearly delineated security roles and responsibilities; performed regular, periodic assessments of risk; implemented security policies and procedures that addressed all aspects of VA's interconnected environment; established an ongoing monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; or instituted a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

In our report to VA, we recommended that the Secretary direct the CIO to (1) work with the other VA CIOs to address all identified computer control weaknesses, (2) develop and implement a comprehensive departmentwide computer security planning and management program, (3) review and assess computer control weaknesses identified throughout the department and establish a process to ensure that these weaknesses are addressed, and (4) monitor and periodically report on the status of improvements to computer security throughout the department.

In commenting on our report, VA agreed with these recommendations and stated that the department would immediately correct the identified computer control weaknesses and implement oversight mechanisms to ensure that these problems do not reoccur. VA also stated that the department was developing plans to correct deficiencies previously identified by the IG and by internal evaluations and that the VA CIO will report periodically on VA's progress in correcting computer control weaknesses throughout the department. We have discussed these actions with VA officials, and, as part of our upcoming review, we will be examining completed actions and evaluating their effectiveness.

WEAKNESSES AT THE SOCIAL SECURITY ADMINISTRATION

The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which, for 1997, included payments that totaled approximately $390 billion to 50 million beneficiaries. This was almost 25 percent of the $1.6 trillion in that year's federal expenditures. SSA also issues social security numbers and maintains earnings records and other personal information on virtually all U. S. citizens. Through its programs SSA processes approximately 225 million wage and tax statements (W-2 forms) annually for approximately 138 million workers. Few federal agencies affect so many people.

The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. In addition, many current beneficiaries rely on the uninterrupted flow of monthly payments to meet their basic needs. In November 1997, the SSA IG reported serious weaknesses in controls over information resources, including access, continuity of service, and software program

changes that unnecessarily place these assets and operations at risk.[6] These weaknesses demonstrate the need for SSA to do more to assure that adequate controls are provided for information collected, processed, transmitted, stored, or disseminated in general support systems or major applications.

Internal control testing identified information protection-related weaknesses throughout SSA's information systems environment. Affected areas included SSA's distributed computer systems as well as its mainframe computers. These vulnerabilities exposed SSA and its computer systems to external and internal intrusion; subjected sensitive SSA information related to social security numbers, earnings, disabilities, and benefits to potential unauthorized access, modification, and/or disclosure; and increased the risks of fraud, waste, and abuse. Access control and other weaknesses also increased the risks of introducing errors or irregularities into data processing operations.

For example, auditors identified numerous employee user accounts on SSA networks, including dial-in modems, that were either not password protected or were protected by easily guessed passwords. These weaknesses increased the risk that unauthorized outsiders could access, modify, and delete data; create, modify, and delete users; and disrupt services on portions of SSA's network. In addition, auditors identified network control weaknesses that could result in accidental or intentional alteration of birth and death records, as well as unauthorized disclosure of personal data and social security numbers.

These weaknesses were made worse because security awareness among employees was not consistent at SSA. As a result, SSA was susceptible to security penetration techniques, such as social engineering, whereby users disclose sensitive information in response to seemingly legitimate requests from strangers either over the phone or in person. The auditors reported that during testing, they were able to secure enough information through social engineering to allow access to SSA's network.

Further, by applying intrusion techniques in penetration tests, auditors gained access to various SSA systems that would have allowed them to view user data, add and delete users, modify network configurations, and disrupt service to users. By gaining access through such tests, auditors also were able to execute software tools that resulted in their gaining access to SSA electronic mailboxes, public mailing lists, and bulletin boards. This access would have provided an intruder the ability to read, send, or change e-mail exchanged among SSA users, including messages from or to the Commissioner.

In addition to access control weaknesses and inadequate user awareness, employee duties at SSA were not appropriately segregated to reduce the risk that an individual employee

---

[6]Social Security Accountability Report for Fiscal Year 1997, SSA Pub. No. 31-231, November 1997.

could introduce and execute unauthorized transactions without detection. As a result, certain employees had the ability to independently carry out actions such as initiating and adjudicating claims or moving and reinstating earnings data. This weakness was exacerbated because certain mitigating monitoring or detective controls could not be relied on. For example, SSA has developed a system that allows supervisors to review sensitive or potentially fraudulent activity. However, key transactions or combinations of transactions are not being reviewed or followed up promptly and certain audit trail features have not been activated.

Weaknesses such as those I have just described increase the risk that a knowledgeable individual or group could fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, such individuals could secretly obtain sensitive information and sell or otherwise use it for personal gain.

The recent growth in "identity theft," where personal information is stolen and used fraudulently by impersonators for purposes such as obtaining and using credit cards, has created a market for such information. According to the SSA IG's September 30, 1997, report to the Congress (included in the SSA's fiscal year 1997 Accountability Report), 29 criminal convictions involving SSA employees were obtained during fiscal year 1997, most of which involved creating fictitious identities, fraudulently selling SSA cards, misappropriating refunds, or abusing access to confidential information. The risk of abuse by SSA employees is of special concern because, except for a very few individuals, SSA does not restrict access to view sensitive data based on a need-to-know basis. As a result, a large number of SSA employees can browse enumeration, earnings, and claims records for many other individuals, including other SSA employees, without detection. SSA provides this broad access because they feel that it facilitates their employees' ability to carry out SSA's mission.

An underlying factor that contributes to SSA's information security weaknesses is inadequate entitywide security program planning and management. Although SSA has an entitywide security program in place, it does not sufficiently address all areas of security, including dial-in access, telecommunications, certain major mainframe system applications, and distributed systems outside the mainframe environment. A lack of such an entitywide program impairs each group's ability to develop a security structure for its responsible area and makes it difficult for SSA management to monitor agency performance in this area.

In two separate letters to SSA management, the IG and its contractor made recommendations to address the weaknesses reported in November 1997. SSA has agreed with the majority of the recommendations and is developing related corrective action plans.

IMPROVEMENTS REQUIRE INDIVIDUAL AGENCY ACTIONS AND STRENGTHENED CENTRAL OVERSIGHT

Substantively improving federal information security will require efforts at both the individual agency level and at the governmentwide level. Agency managers are primarily responsible for securing the information resources that support their critical operations. However, central oversight also is important to monitor agency performance and address crosscutting issues that affect multiple agencies. Over the last 2 years, a number of efforts have been initiated, but additional actions are still needed.

Improved Security Program Management Needed at Individual Agencies

First, it is important that agency managers implement comprehensive programs for identifying and managing their security risks in addition to correcting specific reported weaknesses. Over the last 2 years, our reports and IG reports have included scores of recommendations to individual agencies, and agencies have either implemented or planned actions to address most of the specific weaknesses. However, there has been a tendency to react to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses.

In short, agencies need to move beyond addressing individual audit findings and supplement these efforts with a framework for proactively managing the information security risks associated with their operations. Such a framework includes determining which risks are significant, assigning responsibility for taking steps to reduce risks, and ensuring that these steps are implemented effectively and remain effective over time. Without a management framework for carrying out these activities, information security risks to critical operations may be poorly understood; responsibilities may be unclear and improperly implemented; and policies and controls may be inadequate, ineffective, or inconsistently applied.

Best Practices of Leading Organizations Provide Guidance

In late 1996, at the Committee's request, we undertook an effort to identify potential solutions to this problem, including examples that could supplement existing guidance to agencies. To do this, we studied the security management practices of eight nonfederal organizations known for their superior security programs. These organizations included two financial services corporations, a regional electric utility, a state university, a retailer, a state agency, a computer vendor, and an equipment manufacturer.

We found that these organizations managed their information security risks through a cycle of risk management activities, and we identified 16 specific practices that supported these risk management principles. These practices are outlined in an executive guide titled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), which was released by the Committee in May 1998 and endorsed by

the CIO Council. Upon publication, the guide was distributed to all major agency heads, CIOs and IGs.

The guide describes a framework for managing information security risks through an ongoing cycle of activities coordinated by a central focal point. Such a framework can help ensure that existing controls are effective and that new, more advanced control techniques are prudently and effectively selected and implemented as they become available. The risk management cycle and the 16 practices supporting this cycle of activity are depicted in the following figures.

Figure 1: The Risk Management Cycle

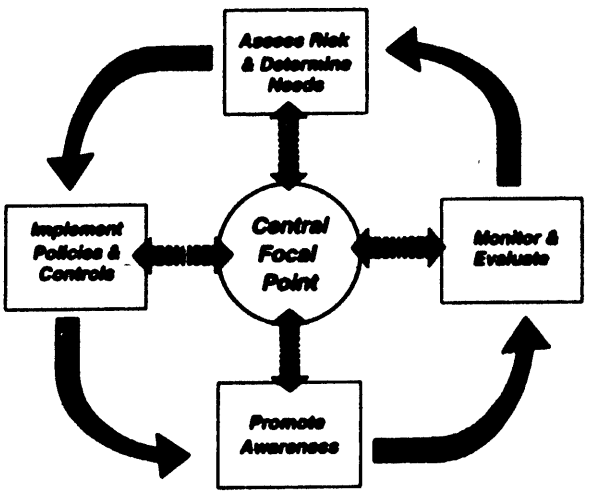
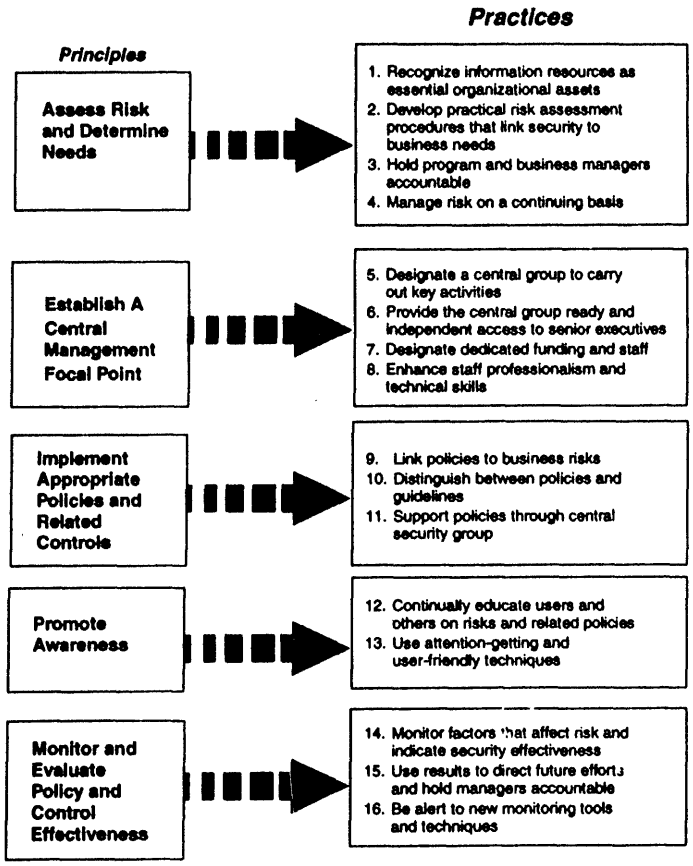


Figure 2: Sixteen Practices Employed by Leading Organizations to Implement the Risk Management Cycle



Centrally Directed Improvement Efforts Have Increased

In addition to effective security program planning and management at individual agencies, governmentwide leadership, coordination, and oversight are important to

- ensure that federal executives understand the risks to their operations,
- monitor agency performance in mitigating these risks,
- ensure implementation of needed improvements, and
- facilitate actions to resolve issues affecting multiple agencies.

To help achieve this, the Paperwork Reduction Act of 1980 made OMB responsible for developing information security policies and overseeing related agency practices. In 1996, we reported that OMB's oversight consisted largely of reviewing selected agency system-related projects and participating in various federal task forces and working groups. While these activities are important, we recommended that OMB play a more active role in overseeing agency performance in the area of information security.

Since then, OMB's efforts have been supplemented by those of the CIO Council. In late 1997, the Council, under OMB's leadership, designated information security as one of six priority areas and established a Security Committee, an action that we had recommended in 1996. The Security Committee, in turn, has established relationships with other federal entities involved in security and developed a very preliminary plan. While the plan does not yet comprehensively address the various issues affecting federal information security or provide a long-range strategy for improvement, it does cover important areas by specifying three general objectives: promote awareness and training, identify best practices, and address technology and resource issues. During the first half of 1998, the committee has sponsored a security awareness seminar for federal agency officials and developed plans for improving agency access to incident response services.

More recently, in May 1998, Presidential Decision Directive (PDD) 63 was issued in response to recommendations made by the President's Commission on Critical Infrastructure Protection in October 1997.[7] PDD 63 established entities within the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation to address critical infrastructure protection, including federal agency information infrastructures. Specifically, the directive states that "the Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved" and that federal department and agency CIOs shall be responsible for

---

[7]Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, October 1997.

information assurance. The directive requires each department and agency to develop a plan within 180 days from the issuance of the directive in May 1998 for protecting its own critical infrastructure, including its cyber-based systems. These plans are then to be subject to an expert review process. Other key provisions related to the security of federal information systems include

- a review of existing federal, state, and local bodies charged with information assurance tasks;
- enhanced collection and analysis of information on the foreign information warfare threat to our critical infrastructures;
- establishment of a National Infrastructure Protection Center within the Federal Bureau of Investigation to facilitate and coordinate the federal government's investigation and response to attacks on its critical infrastructures;
- assessments of U. S. government systems' susceptibility to interception and exploitation; and
- incorporation of agency infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

We plan to follow up on the these activities as more specific information becomes available.

A COMPREHENSIVE AND COORDINATED GOVERNMENTWIDE STRATEGY NEEDS TO EMERGE

The CIO Council's efforts and the issuance of PDD 63 indicate that senior federal officials are increasingly concerned about information security risks and are acting on these concerns. Improvements are needed both at the individual agency level and in central oversight, and coordinated actions throughout the federal community will be needed to substantively improve federal information security.

What needs to emerge is a coordinated and comprehensive strategy that incorporates the worthwhile efforts already underway and takes advantage of the expanded amount of evidence that has become available in recent years. The objectives of such a strategy should be to encourage agency improvement efforts and measure their effectiveness through an appropriate level of oversight. This will require a more structured approach for (1) ensuring that risks are fully understood, (2) promoting use of the most cost-effective control techniques, (3) testing and evaluating the effectiveness of agency programs, and (4) acting to address identified deficiencies. This approach needs to be applied at individual departments and agencies and in a coordinated fashion across government.

In our report on governmentwide information security that is being released today, we recommended that the Director of OMB and the Assistant to the President for National Security Affairs develop such a strategy. As part of our recommendation, we stated that such a strategy should

- ensure that executive agencies are carrying out the responsibilities outlined in laws and regulations requiring them to protect the security of their information resources;
- clearly delineate the roles of the various federal organizations with responsibilities related to information security;
- identify and rank the most significant information security issues facing federal agencies;
- promote information security risk awareness among senior agency officials whose critical operations rely on automated systems;
- identify and promote proven security tools, techniques, and management best practices;
- ensure the adequacy of information technology workforce skills;
- ensure that the security of both financial and nonfinancial systems is adequately evaluated on a regular basis;
- include long-term goals and objectives, including time frames, priorities, and annual performance goals; and
- provide for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

In commenting on a draft of our report, the OMB's Acting Deputy Director for Management said that a plan is currently being developed by OMB and the CIO Council, working with the National Security Council. The comments stated that the plan is to develop and promote a process by which government agencies can (1) identify and assess their existing security posture, (2) implement security best practices, and (3) set in motion a process of continued maintenance. The comments also describe plans for a CIO Council-sponsored interagency assist team that will review agency security programs. As of September 17, a plan had not yet been finalized and, therefore, was not available for our review, according to an OMB official involved in the plan's development. We intend to review the plan as soon as it is available.

YEAR 2000 CRISIS INCREASES SENSE OF URGENCY FOR IMPROVED SECURITY

Although information security, like other types of safeguards and controls, is an ongoing concern, it is especially important, now and in the coming 18 months, as we approach and deal with the computer problems associated with the Year 2000 computing crisis. The Year 2000 crisis presents a number of security problems with which agencies must be prepared to contend.

For example, it is essential that agencies improve the effectiveness of controls over their software development and change process as they implement the modifications needed to make their systems Year 2000 compliant. Many agencies have significant weaknesses in this area, and most are under severe time constraints to make needed software changes. As a result, there is a danger that already weak controls will be further diminished if agencies bypass or truncate them in an effort to speed the software modification process. This increases the risk that erroneous or malicious code will be implemented or that systems that do not adequately support agency needs will be rushed into use.

Also, agencies should strive to improve their abilities to detect and respond to anomalies in system operations that may indicate unauthorized intrusions, sabotage, misuse, or damage that could affect critical operations and assets. As illustrated by VA and SSA, many agencies are not taking full advantage of the system and network monitoring tools that they already have and many have not developed reliable procedures for responding to problems once they are identified. Without such incident detection and response capabilities, agencies may not be able to readily distinguish between malicious attacks and system-induced problems, such as those stemming from Year 2000 noncompliance, and respond appropriately.

The Year 2000 crisis is the most dramatic example yet of why we need to protect critical computer systems because it illustrates the government's widespread dependence on these systems and the vulnerability to their disruption. However, the threat of disruption will not end with the advent of the new millennium. There is a longer-term danger of attack from malicious individuals or groups, and it is important that our government design long-term solutions to this and other security risks.

- - - - - - - - - - - - - - - - - - -

Mr. Chairman, this concludes our statement. We would be happy to respond to any questions you or other members of the Committee may have.

Statement by

Harold F. Gracey, Jr.

Acting Assistant Secretary for Information and Technology

Department of Veterans Affairs

Before the

United States Senate

Committee on Governmental Affairs

September 23, 1998

Good morning, Mr. Chairman and members of the Committee. I am pleased to testify before you today to discuss computer security issues at the Department of Veterans Affairs.

The Department provides services to veterans and their families. These benefits primarily are for veterans in the form of Compensation, Pension and Education programs through Regional Offices; in the form of medical care and services through medical centers, domiciliaries and outpatient clinics; and in the form of graveside and burial services for deserving veterans and qualifying family members. VA operates from almost 1200 facilities across the nation, employing approximately two hundred nineteen thousand employees. There are approximately seventy million persons who are veterans, dependents and survivors of deceased veterans who are potentially eligible for VA benefits and services.

To facilitate these services, VA has extensive computer system networks and electronic information. The systems are generally aligned with each major administration within VA: the Veteran Benefits Administration, the Veteran Health Administration, and the National Cemetery System. Additionally, Departmental administrative systems which support all elements of VA are supported through a large centralized service center. While much of VA information is contained in what may be considered "legacy" systems, all of the information centers are interconnected so that limited critical forms of information may be exchanged among various sites and information applications. This information is not classified as secret information, but is highly sensitive since it includes personal information about a large body of the nation's population. In addition to information about veteran programs, VA has virtually completed implementation of an integrated administrative E-mail network which permits seamless exchange of electronic mail across the breadth of the Department.

We have recently experienced several General Accounting Office (GAO) and VA Office of Inspector General (OIG) reviews of our information technology security. There are a number of findings which identify vulnerabilities and needed improvements at specific sites, among specific organizations, and in VA wide security program management. We do not dispute the GAO and OIG findings, and have already acted upon most of their recommendations. We have contracted for third party reviews of our major centers in the past, and despite our concerns with continuing vulnerabilities, we view the recent reports as providing us an opportunity to strengthen our information security program with a more comprehensive computer security planning and management program.

We intend to address each of the recommendations identified by the GAO and VA's OIG in their four recent reviews, including VA's:

- control and oversight of access to its systems;
- protection of VA systems from unauthorized access from remote locations or through the VA network;
- performance of regular periodic assessments of risk; and
- development and implementation of a comprehensive department-wide computer security planning and management program.

As GAO indicates, VA immediately corrected the identified computer control weaknesses and implemented oversight mechanisms to ensure that these problems do not re-occur. In September 1998, my office finalized with the full participation of the respective Administration Chief Information Officers a detailed **Integrated VA Security Plan** for implementing each of the recommendations. Each VA Administration is responsible to complete a specific series of tasks structured to correct deficiencies. Plan status and progress will be provided monthly to the OIG. The projected date of completion for the tasks in this plan is December 1998.

We also have prepared a **Draft VA Information Technology Security Program Plan** that addresses department-wide computer security issues, including policies, guidance and procedures and responsibilities. This plan addresses the recent reports, as well as

other program shortcomings. It is expected to create more explicit guidance to VA Administrations with increased oversight requirements.

I am committed to a strong information technology security program, and I intend to ensure security receives adequate attention with an elevated level of scrutiny in VA.

I appreciate the opportunity to address this important matter and will be pleased to answer any questions you may have.

FOR RELEASE UPON DELIVERY

COMPUTER SECURITY AT THE SOCIAL SECURITY ADMINISTRATION

STATEMENT BY

JOHN R. DYER
PRINCIPAL DEPUTY COMMISSIONER OF SOCIAL SECURITY

BEFORE THE
COMMITTEE ON GOVERNMENTAL AFFAIRS

SEPTEMBER 23, 1998

Mr. Chairman and Members of the Committee:

Thank you for inviting me here today to discuss computer security at the Social Security Administration (SSA).

At the outset, Mr. Chairman, it is our highest priority to maintain the confidentiality of the information in SSA's systems. Nothing is more important in the operation of our programs than ensuring that the public has confidence that the information placed in our trust is secure. This basic philosophy is a cornerstone of everything we do. In fact, the very first regulation issued by the new Social Security Administration in 1935 dealt with the nondisclosure of SSA record data.

SSA pays benefits each month to almost 50 million beneficiaries. In FY 1998 alone, SSA delivered $400 billion in benefits. In order to achieve our mission, many of Social Security's 66,000 employees must have access, on a need to know basis, to computer records. This creates an inherent tension between the need to deliver accurate benefits on time to the right person and the need to have the tightest security possible. When the agency learns that an employee has abused his or her systems privileges, steps are immediately taken to impose penalties, as severe as termination, on the individual.

When Social Security first became independent in 1995, and had its own Inspector General (IG) for the first time devoted only to SSA's activities, the Commissioner asked the IG to make employee integrity the number one issue and the IG has done so. SSA has consistently asked for additional resources for the IG and received support from Congress for those requests.

We have taken both preventive and enforcement actions to protect information in Social Security files from any wrongful use by our own employees and from any unauthorized access by outsiders. It is important to emphasize that SSA's mainframe computers have never been successfully penetrated by outside parties. This is not to say that we are resting on our laurels. We constantly reevaluate and, when necessary, upgrade the security features necessary to maintain the public's confidence that our systems are secure.

Maintaining SSA Systems Security

In order to meet the challenges of data security in today's highly technological environment, the Agency has adopted an enterprise-wide approach to systems security, financial information, data integrity, and prevention of fraud, waste, and

abuse. We have full-time staff devoted to systems security stationed throughout the Agency, in all regions and in central office. They provide day to day oversight and control over our computer software. In addition, we have a Deputy Commissioner-level Office of Systems which supports the operating system, develops new software and the related controls and in general assures that SSA is taking advantage of the latest in effective systems technology.

SSA has a Chief Financial Officer, also at the Deputy Commissioner–level, who assures that all new systems have the required financial controls to maintain sound stewardship over the monies entrusted to our care. In addition, as the Principal Deputy Commissioner, I also serve as the agency's Chief Information Officer; this dual role gives me the oversight of the agency as a whole to assure that our initiatives are enterprise wide in scope.

As I have mentioned, as an independent agency, we have our own IG who can focus his efforts on the agency's needs and concerns. The IG is also very active in working with other Federal, State and local law enforcement agencies to assure all avenues for investigation and prosecution are being pursued--especially for systems security-related issues.

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

In summary, we have in place the right authorities, the right personnel, and the right software controls to prevent penetration of our systems and to address systems security issues as they surface.

Audit of SSA's Systems Controls

SSA, as an agency, has been preparing audited financial statements since FY 1987. Fiscal year 1997 represented the fourth consecutive year that SSA's financial statements have received an unqualified, or clean, audit opinion from SSA's IG or its contractor. The auditors stated, "In our opinion management's assertion that SSA's systems of accounting and internal controls are in compliance with the internal control objectives in OMB Bulletin NO. 93-06 is fairly stated, in all material respects". SSA received an unqualified opinion from the auditors that our systems of internal controls meet the standards set up by the Office of Management and Budget (OMB). Our financial statements are prepared consistent with the requirements of the Federal Accounting Standards Advisory Board, OMB, the Chief Financial Officers' Act, and other relevant Federal statutes.

PricewaterhouseCoopers (PwC) conducted the FY 1997 audit under contract with the General Accounting Office (GAO) and our IG. As part of the audit, PwC provided SSA with two management letters that gave recommendations as to how SSA could improve its systems safeguards and financial management controls. Over the past few months, SSA and PwC have been working closely to reach final agreement on how to achieve the objectives of the PwC recommendations. (We have provided this committee with SSA's FY 1997 financial statement--part of the latest Accountability Report--as well as two Management Letters given to SSA by PwC.)

SSA's Response to the Audit

The Social Security Administration and our auditor, PwC, are in agreement on almost all recommendations. SSA takes these issues seriously and has embarked on an aggressive timetable of corrective action. Some of the auditor's recommendations take longer to achieve but I believe that the auditor would say that we are proceeding expeditiously. SSA and PwC have come to closure on virtually all of the recommendations contained in the PwC reports. PwC is now reviewing our progress in making the called for changes and will report on them as part of the audit of SSA's financial statements for fiscal year 1998, this fall.

SSA has developed a workplan to implement these agreed-upon improvements. There are a couple of areas where we are still exploring solutions and expect to close them out as part of the FY 1998 audit process.

I would like now to address some of the major changes we are making in the four primary areas that PwC identified as follows:

1) SSA needs improved controls to protect its information;

2) SSA needs to improve and fully test its plan for maintaining continuity of operations;

3) SSA needs to improve its software application development and change control policies and procedures; and

4) SSA needs to improve controls over insufficient separation of duties.

Finding 1, Protection of Information: The auditors made 43 recommendations on how the Agency could better protect its data in both a mainframe and distributive environment. We agreed with 41 of these recommendations and have closed or completed 30 to date. Some of the actions taken include limiting the use of modems, implementing a process to identify unauthorized modems on a continuing basis, removing access immediately for unauthorized modems when discovered; and strengthening access controls over programmers and other system's personnel. New password guidelines were implemented which require the use of more characters and we are making enhancements to our single sign-on architecture.

The auditors recently told us that they noted improvements in this area in this year's audit, particularly in the mainframe environments, but believed we needed to give more attention to the distributive environment. We will continue working with the auditors to further improve this area.

Finding 2, continuity of operations: There were five recommendations in this area, focused primarily on an updated contingency plan covering both data center activities and activities performed by end users, covering critical operations should interruptions occur, and testing combinations of multiple critical workloads simultaneously. We agreed with all five recommendations.

SSA is committed to testing all critical workloads within a 3-year cycle and has expanded our test capability from 64 hours to 120 hours in 1999. We are taking a fresh look at identifying our critical work loads and how we will maintain continuity of operations in the event of the loss of our computer center in both a short and long-term scenario.

Finding 3, software development: In this area the auditors felt that control and security measures for application systems changes could be improved. We have closed or completed 17 of the 35 recommendations to date and are actively working on the others. New and revised procedures were developed to ensure that requested changes to systems were properly approved, coded, tested, documented, and authorized for production. We now have appropriate policies and procedures in place to document system change control practices and are committed to ensuring 100 percent compliance with policy.

Finding 4, separation of duties: There were three areas where the auditors felt we had inadequate separation of duties: field offices, systems operations, and security administration. We generally agreed that we could improve in the areas of systems operations and security administration and have addressed 18 recommendations so far. We disagreed with five recommendations pertaining to field offices because of the high cost of implementing these recommendations and asked the auditors to reconsider and develop alternative approaches. The auditors have reconsidered these recommendations and are in the process of developing revised recommendations which will emphasize the use of performance measurement data to identify high-risk transactions for analysis and, when warranted, additional preventive controls. These new recommendations are much less labor intensive and appear to be achievable. We will continue to work with the auditors to improve this area.

I want to come back to the broader concerns. Addressing systems security is and always will be first of all a high priority for SSA. By design, the Agency has used a system architecture that relied almost exclusively on mainframe systems and centralized databases. With this architecture we are able to more tightly control computer security than those Agencies who are faced with large numbers of local and/or distributed systems.

As SSA, in the increasingly technological environment, moves away from the mainframe environment to more distributed systems, we need to carefully consider at every step of the process how to build in security features. We have already taken a number of steps to ensure that these new systems will be as secure as possible.

We have supported and will continue to support the independent audit of our financial statements. We have supported the auditors detailed testing of SSA's systems. We will work with the various oversight bodies–the General Accounting

Office and the IG, for example, to review what we are doing and identify any issues they believe we need to address. Only in this way can we be assured SSA is getting all the advice that is available to us, and doing its utmost to maintain the security of our computer systems, and the data they contain.

Zero Tolerance for Fraud

Finally, I also want to state that we have a zero tolerance at SSA for fraud, waste, and abuse. We believe that our zero tolerance policy has paid off, as evidenced by the fact that almost all of the recommendations made to the Agency by independent auditors in recent years have been of a theoretical nature, e.g., our systems have a weakness that needs to be addressed to assure there is no abuse. Nonetheless, when we have evidence of an abuse of system privileges, addressing the matter is a number one priority of the Agency.

On June 22, 1998, Commissioner Apfel issued a notice to all SSA employees about administrative sanctions to be taken against any SSA employee who abuses his or her systems privileges. The penalties are severe and will lead to termination of employment for any offense that involves selling data.

SSA's IG is committed to the investigation and prosecution of every employee abuse case that is identified. Many of the SSA employee cases turned over to the Inspector General for investigation were first discovered by the Social Security Administration itself. In addition, we have asked the IG to make investigation of employee fraud the number one priority.

Conclusion

As I noted at the outset the Social Security Administration has a long-standing tradition of assuring the public that their personal records are secure. Systems security is not a one-time task to be accomplished, but rather is an ongoing mission we can never lose sight of. We know we cannot rest on past practice, but must be vigilant in every way we can to assure that these personal records remain secure, and that public confidence in SSA is maintained.

I want to thank the Committee for holding this hearing and focusing on what we all view as a critical issue. We are glad to know that the Congress shares our concerns, and we will work with the Committee to assure the American people that we are doing all we can to maintain the security of our computer operations.

This concludes my prepared statement. I will be happy to answer any questions you may have.

United States General Accounting Office

GAO

Report to the Secretary of Veterans Affairs

September 1998

INFORMATION SYSTEMS

VA Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure

GAO/AIMD-98-175

GAO

United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-280049

September 23, 1998

The Honorable Togo D. West, Jr.
The Secretary of Veterans Affairs

Dear Mr. Secretary:

This report discusses weaknesses that we identified during our assessment of general computer controls that support key financial management and benefit delivery operations of the Department of Veterans Affairs (VA). General computer controls affect the overall effectiveness and security of computer operations as opposed to being unique to any specific computer application. They include security management, operating procedures, software security features, and physical protection designed to ensure that access to data is appropriately restricted, only authorized changes are made to computer programs, computer security duties are segregated, and backup and recovery plans are adequate to ensure the continuity of essential operations. Such controls are critical to VA's ability to safeguard assets, maintain the confidentiality of sensitive financial data and information on veteran medical records and benefit payments, and ensure the reliability of financial management information.

Our review of VA's general computer controls was performed in connection with the department's financial audit conducted under the Chief Financial Officers Act of 1990, as expanded by the Government Management Reform Act of 1994. The results of our evaluation of general computer controls were shared with VA's Office of Inspector General (OIG) for its use in auditing VA's consolidated financial statements for fiscal year 1997.

This report does not detail certain serious weaknesses in controls over access to VA computer resources. A separate report on those matters, with limited distribution due to its sensitive nature, is being issued today.

Results in Brief

General computer control weaknesses place critical VA operations, such as financial management, health care delivery, benefit payments, life insurance services, and home mortgage loan guarantees, and the assets associated with these operations, at risk of misuse and disruption. In addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical

records and benefit payments, is vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction, possibly occurring without detection. The general control weaknesses we identified could also diminish the reliability of the department's financial statements and other management information derived from VA's systems.

We found significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit the access of authorized users or effectively manage user identifications (ID) and passwords. The department also had not established effective controls to prevent individuals, both internal and external, from gaining unauthorized access to VA systems. VA's access control weaknesses were further compounded by ineffective procedures for overseeing and monitoring systems for unusual or suspicious access activities.

In addition, the department was not providing adequate physical security for its computer facilities, assigning duties in such a way as to segregate incompatible functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to prepare its computer operations to maintain or regain critical functions in emergency situations. Many of these access and other general computer control weaknesses are similar to weaknesses that have been previously identified by VA's OIG and consultant evaluations. Also, the OIG reported information system security controls as a material weakness in its report on VA's consolidated financial statements for fiscal year 1997.

A primary reason for VA's continuing general computer control problems is that the department does not have a comprehensive computer security planning and management program. An effective program would include guidance and procedures for assessing risks, establishing appropriate policies and related controls, raising awareness of prevailing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls. Such a program, if implemented completely across the department, would provide VA with a solid foundation for resolving existing computer security problems and managing its information security risks on an ongoing basis.

The VA facilities that we visited plan to address all of the specific computer control weaknesses identified. In fact, the director of the Austin Automation Center told us that his staff had corrected many of the general computer control weaknesses that we identified. The director of the Dallas Medical Center and the Veterans Benefits Administration Chief

Information Officer (CIO) also said that specific actions had been taken to correct the computer control weaknesses that we identified at the Dallas Medical Center and the Hines and Philadelphia benefits delivery centers. Furthermore, the Deputy Assistant Secretary for Information Resources Management told us that VA plans to develop a comprehensive security plan and management program.

Background

VA provides health care and other benefits to veterans in recognition of their service to our country. As of July 1, 1997, 26 percent of the nation's population—approximately 70 million persons who are veterans, veterans' dependents, or survivors of deceased veterans—was potentially eligible for VA benefits and services, such as health care delivery, benefit payments, life insurance protection, and home mortgage loan guarantees.

VA operates the largest health care delivery system in the United States and guarantees loans on about 20 percent of the homes in the country. In fiscal year 1997, VA spent more than $17 billion on medical care and processed more than 40 million benefit payments totaling more than $20 billion. The department also provided life insurance protection through more than 2.5 million policies that represented about $24 billion in coverage at the end of fiscal year 1997.

In providing these benefits and services, VA collects and maintains sensitive medical record and benefit payment information for millions of veterans and their dependents and survivors. VA also maintains medical information for both inpatient and outpatient care. For example, the department records admission, diagnosis, surgical procedure, and discharge information for each stay in a VA hospital, nursing home, or domiciliary. VA also stores information concerning health care provided to and compensation received by ex-prisoners of war. In addition, VA maintains information concerning each of the guaranteed or insured loans closed by VA since 1944, including about 3.5 million active loans.

VA relies on a vast array of computer systems and telecommunication networks to support its operations and store the sensitive information it collects in carrying out its mission. Three centralized data centers—located in Austin, Texas; Hines, Illinois; and Philadelphia, Pennsylvania—maintain the department's financial management systems; process compensation, pension, and other veteran benefit payments; and manage the veteran life insurance programs. In addition to the three centralized data centers, the Veterans Health Administration (VHA)

operates 172 hospitals at locations across the country that operate local financial management and medical support systems on their own computer systems.

The Austin Automation Center maintains VA's departmentwide systems, including centralized accounting, payroll, vendor payment, debt collection, benefits delivery, and medical systems. In fiscal year 1997, VA's payroll was almost $11 billion and the centralized accounting system generated more than $7 billion in additional payments. The Austin Automation Center also provides, for a fee, information technology services to other government agencies. The center currently processes a workers compensation computer application for other federal agencies and plans to expand the computing services it provides to federal agencies.

The other two centralized data centers support VA's Veterans Benefits Administration (VBA) programs. The Hines Benefits Delivery Center processes information from VA systems that support the compensation, pension, and education applications for VBA's 58 regional offices The Philadelphia Benefits Delivery Center is primarily responsible for supporting VA's life insurance program.

In addition, VHA hospitals operate local financial management and medical support systems on their own computer systems. The medical support systems manage information on veteran inpatient and outpatient care, as well as admission and discharge information, while the main medical financial system—the Integrated Funds Distribution, Control Point Activity, Accounting and Procurement (IFCAP) system—controls most of the $17 billion in funds that VA spent on medical care in fiscal year 1997. The IFCAP system also transmits financial and inventory information daily to the Financial Management System in Austin.

The three VA data centers, as well as the 172 VHA hospitals, 58 VBA regional offices, and the VA headquarters office, are all interconnected through a wide area network. All together, VA's network serves more than 40,000 on-line users.

Objective, Scope, and Methodology

Our objective was to evaluate and test the effectiveness of general computer controls over the financial systems maintained and operated by VA at its Austin, Hines, and Philadelphia data centers as well as selected VA medical centers. General computer controls, however, also affect the

security and reliability of nonfinancial information, such as veteran medical, loan, and insurance data, maintained at these processing centers.

At the Austin Automation Center and VA medical centers in Dallas and Albuquerque, we evaluated controls intended to

- protect data and application programs from unauthorized access;
- prevent the introduction of unauthorized changes to application and system software;
- provide segregation of duties involving application programming, system programming, computer operations, security, and quality assurance;
- ensure recovery of computer processing operations in case of a disaster or other unexpected interruption; and
- ensure that an adequate computer security planning and management program is in place.

The scope of our work at the Hines and Philadelphia benefits delivery centers was limited to (1) evaluating the appropriateness of access granted to selected individuals and computer resources, (2) assessing efforts to monitor access activities, and (3) examining the computer security administration structure. We restricted our evaluation at the Hines and Philadelphia benefits delivery centers because VA's OIG was planning to perform a review of other general computer controls at these sites during fiscal year 1997.

To evaluate computer controls, we identified and reviewed VA's information system general control policies and procedures. Through this review and discussions with VA staff, including programming, operations, and security personnel, we determined how the general computer controls were intended to work and the extent to which center personnel considered them to be in place. We also reviewed the installation and implementation of VA's operating system and security software.

Further, we tested and observed the operation of general computer controls over VA's information systems to determine whether they were in place, adequately designed, and operating effectively. To assist in our evaluation and testing of general computer controls, we contracted with Ernst & Young LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

We performed our work at the VA data centers in Austin, Hines, and Philadelphia; the VA medical centers in Dallas and Albuquerque; and VA headquarters in Washington, D.C., from October 1997 through January 1998. Our work was performed in accordance with generally accepted government auditing standards.

VA provided us with written comments on a draft of this report, which are discussed in the "Agency Comments" section and reprinted in appendix I.

Access to Data and Programs Is Not Adequately Controlled

A basic management objective for any organization is to protect data supporting its critical operations from unauthorized access, which could lead to improper modification, disclosure, or deletion. Our review of VA's general computer controls found that the department was not adequately protecting financial and sensitive veteran medical and benefit information. Specifically, VA did not adequately limit the access granted to authorized VA users, properly manage user IDs and passwords, or routinely monitor access activity. As a result, VA's computer systems, programs, and data are at risk of inadvertent or deliberate misuse, fraudulent use, and unauthorized alteration or destruction occurring without detection.

We also found that VA had not adequately protected its systems from unauthorized access from remote locations or through the VA network. The risks created by these security issues are serious because in VA's interconnected environment, the failure to control access to any system connected to the network also exposes other systems and applications on the network. Due to the sensitive nature of the remote access and network control weaknesses we identified, these issues are described in a separate report with limited distribution issued to you today.

Access Authority Is Not Appropriately Limited for Authorized VA Users

A key weakness in VA's internal controls was that the department was not adequately limiting the access of VA employees. Organizations can protect information from unauthorized changes or disclosures by granting employees authority to read or modify only those programs and data that are necessary to perform their duties.

VA, however, allowed thousands of users to have broad authority to access financial and sensitive veteran medical and benefit information. At Austin, for example, the security software was implemented in a manner that provided all of the more than 13,000 users with the ability to access and change sensitive data files, read system audit information, and execute

powerful system utilities. Such broad access authority increased the risk that users could circumvent the security software, and presented users with an opportunity to alter or delete any computer data or program. The director of the Austin Automation Center told us that his staff had restricted access to the sensitive data files, system audit information, and powerful system utilities that we identified.

In addition, we found several other examples where VA did not adequately restrict the access of legitimate users, including the following.

- At both the Hines and Philadelphia centers, we found that system programmers had access to both system software and financial data. This access could allow the programmers to make changes to financial information without being detected.
- At the Hines center, we also identified 18 users in computer operations who could update sensitive computer libraries. Update access to these libraries could result in the security software being circumvented with the use of certain programs to alter or delete sensitive data.
- At the Dallas center, we determined that 12 computer support personnel had access to all financial and payroll programs and data. Although these support staff need access to certain programs, providing complete access weakens the organization's ability to ensure that only authorized changes are allowed.
- At the Austin center, we found more than 100 users who had an access privilege that provided the ability to bypass security controls and enabled them to use any command or transaction. Access to this privilege should be limited to use in emergencies or for special purposes because it creates a potential security exposure.

The director of the Austin Automation Center told us that the privilege that provided users the opportunity to bypass security controls had been removed from all individual user IDs. The VBA CIO also said that a task force established to address control weaknesses had evaluated the inappropriate access that we identified at the Hines and Philadelphia benefits delivery centers and made recommendations for corrective measures.

We also found that VA was not promptly removing access authority for terminated or transferred employees or deleting unused or unneeded IDs.

- At the Dallas and Albuquerque centers, we found that IDs belonging to terminated and transferred employees were not being disabled. We

identified over 90 active IDs belonging to terminated or transferred employees at Dallas and 50 at Albuquerque. If user IDs are not promptly disabled when employees are terminated, former employees are allowed the opportunity to sabotage or otherwise impair VA operations.

- At the Dallas center, we identified more than 800 IDs that had not been used for at least 90 days. We also identified inactive IDs at the Austin, Hines, and Albuquerque centers. For instance, at the Hines center, we found IDs that had been inactive for as long as 7 years. Allowing this situation to persist poses unnecessary risk that unneeded IDs will be compromised to gain unauthorized access to VA computer systems.

In January 1998, the director of the Dallas Medical Center said that a program had been implemented to disable all user IDs for terminated employees and those IDs not used in the last 90 days. In addition, the director of the Austin Automation Center and the VBA CIO told us that IDs would be automatically suspended 30 days after the password expired at the Austin, Hines, and Philadelphia centers.

One reason that VA's user access problems existed was because user access authority was not being reviewed periodically. Such periodic reviews would have allowed VA to identify and correct inappropriate access.

The directors of the Austin Automation Center and the Dallas Medical Center told us that they planned to periodically review system access. The VBA CIO also said that the Hines and Philadelphia benefits delivery centers will begin routinely reviewing user IDs and deleting individuals accordingly.

User ID and Password Management Controls Are Not Effective

In addition to overseeing user access authority, it is also important to actively manage user IDs and passwords to ensure that users can be identified and authenticated. To accomplish this objective, organizations should establish controls to maintain individual accountability and protect the confidentiality of passwords. These controls should include requirements to ensure that IDs uniquely identify users; passwords are changed periodically, contain a specified number of characters, and are not common words; default IDs and passwords are changed to prevent their use; and the number of invalid password attempts is limited. Organizations should also evaluate the effectiveness of these controls periodically to ensure that they are operating effectively. User IDs and passwords at the sites we visited were not being effectively managed to

ensure individual accountability and reduce the risk of unauthorized access.

VA had issued an updated security policy in January 1997 that addressed local area network user ID and password management. Specifically, this policy required users to have separate IDs; passwords to be changed periodically, be at least six characters in length, and be formed with other than common words; and IDs to be suspended after three invalid password attempts. Despite these requirements, we identified a pattern of network control weaknesses because VA did not periodically review local area network user IDs and passwords for compliance with this policy.

- At the Albuquerque center, we identified 119 network IDs that were allowed to circumvent password change controls, 15 IDs that did not have any passwords, and eight IDs that had passwords with less than six characters.
- At the Philadelphia center, we found that approximately half of the network user IDs, including the standard network administrator ID, were vulnerable to abuse because passwords were common words that could be easily guessed or found in a dictionary.
- At the Austin and Dallas centers, we found that network passwords were set to never expire. Not requiring passwords to be changed increases the risk that they will be uncovered, which could lead to unauthorized access.

In February 1998, the VBA CIO told us that the Hines and Philadelphia benefits delivery centers plan to require that passwords not be common words. Additionally, the directors of both the Austin Automation Center and the Dallas Medical Center said that although their staffs did not control wide area network password management controls, they were working with VA technical staff to improve network password management by requiring passwords to be changed periodically.

In addition, VA's user ID and password management policy only applied to local area networks. VA did not have departmentwide policies governing user IDs and passwords for other computer platforms, such as mainframe computers or the wide area network. Although some organizations within VA had procedures in these areas, we identified a number of user ID and password management problems.

- At the Philadelphia center, we found that the security software was implemented in a manner that did not disable the master security administration ID after a specified number of invalid password attempts.

Allowing unlimited password attempts to this ID, which has the highest level security authority, increases the risk of unauthorized access to or disclosure of sensitive information.

- At the Austin center, we determined that more than 100 mainframe IDs that did not require passwords, many of which had broad access authority, were not properly defined to prevent individuals from using them. Although system IDs without passwords are required to perform certain operational tasks, these IDs should not be available to individual users because IDs that do not require password validation are more susceptible to misuse. Twenty of these IDs were especially vulnerable to abuse because the account identifiers were common words, software product names, or derivations of words or products that could be easily guessed.
- At the Dallas and Albuquerque centers, we discovered that an ID established by a vendor to handle various support functions had remained active even though the vendor had recommended that this ID be suspended when not in use.

The director of the Austin Automation Center told us that his staff had deleted nearly 50 of the mainframe IDs that did not require passwords and reduced the access authority for many of the remaining IDs that did not require passwords. In addition, the chief of the Information Resources Management Service at the Dallas Medical Center agreed to take steps to address the system maintenance ID problem we identified.

We also found numerous instances where user IDs and passwords were being shared by staff. For example, as many as 16 users at the Albuquerque Medical Center and an undetermined number at the Dallas Medical Center were sharing IDs with privileges to all financial data and system software. At Austin, more than 10 IDs with high-level security access were being shared by several staff members. The use of shared IDs and passwords increases the risk of a password being compromised and undermines the effectiveness of monitoring because individual accountability is lost.

The director of the Austin Automation Center told us that shared IDs had been eliminated and replaced with individually assigned user IDs. In addition, the chief of the Information Resources Management Service at the Dallas Medical Center agreed to take steps to address the shared ID problem we identified.

Access Activities Are Not Being Monitored

The risks created by these access control problems were also heightened significantly because the sites we visited were not adequately monitoring

system and user access activity. Routinely monitoring the access activities of employees, especially those who have the ability to alter sensitive programs and data, can help identify significant problems and deter employees from inappropriate and unauthorized activities. Without these controls, VA had little assurance that unauthorized attempts to access sensitive information would be detected.

Because of the volume of security information that must be reviewed, the most effective monitoring efforts are those that target specific actions. These monitoring efforts should include provisions to review

- unsuccessful attempts to gain entry to a system or access sensitive information,
- deviations from access trends,
- successful attempts to access sensitive data and resources,
- highly-sensitive privileged access, and
- access modifications made by security personnel.

For VA, such an approach could be accomplished using a combination of the audit trail capabilities of its security software and developing computerized reports. This approach would require each facility to compile a list of sensitive system files, programs, and software so that access to these resources could be targeted. Access reports could then be developed for security staff to identify unusual or suspicious activities. For instance, the reports could provide information on browsing trends or summarizations based on selected criteria that would target specific activities, such as repeated attempts to access certain pay tables or sensitive medical and benefit information.

Despite the thousands of employees who had legitimate access to VA computer systems containing financial and operational data, VA did not have any departmentwide guidance for monitoring successful and unsuccessful attempts to access system files containing key financial information or sensitive veteran data. As a result, VA's monitoring efforts were not effective for detecting unauthorized access to or modification of sensitive information.

The security staffs at the Philadelphia, Hines, Dallas, and Albuquerque centers were not actively monitoring access activities. At the Philadelphia center, available violation reports were not being reviewed, while at the Hines center, it was unclear who had specific responsibility for monitoring access. As a result, no monitoring was being performed at either the Hines

or Philadelphia centers. In addition, neither the Dallas nor Albuquerque centers had programs to actively monitor access activities.

Also, violation reports at the Austin Automation Center did not target most types of unusual or suspicious system activity, such as repeated attempts to access sensitive files or libraries or attempts to access certain accounts or pay tables. In addition, the Austin Automation Center had not developed any browsing trends or instituted a program to monitor staff access, particularly access by staff who had significant access authority to critical files, programs, and software.

The director of the Austin Automation Center told us that he plans to establish a new security staff that will be responsible for establishing a targeted monitoring program to identify access violations, ensure that the most critical resources are properly audited, and periodically review highly privileged users, such as system programmers and security administrators. Also, the director of the Dallas Medical Center told us that his staff plan to periodically review user access. In addition, the chief of the Information Resources Management Service told us during follow-up discussions that the Dallas Medical Center will establish a targeted monitoring program to review access activities.

Furthermore, none of the five sites we visited were monitoring network access activity. Although logging events on the network is the primary means of identifying unauthorized users or unauthorized usage of the system by authorized users, two of the sites we reviewed were not logging network security events. Unauthorized network access activity would also go undetected at the sites that were logging network activity because the network security logs were not reviewed.

The director of the Austin Automation Center told us that his staff planned to begin a proactive security monitoring program that would include identifying and investigating unauthorized attempts to gain access to Austin Automation Center computer systems and improper access to sensitive information on these systems. The director of the Dallas Medical Center also told us that his staff planned to implement an appropriate network monitoring program.

Other General Controls Are Not Sufficient

In addition to these general access controls, there are other important controls that organizations should have in place to ensure the integrity and reliability of data. These general computer controls include policies, procedures, and control techniques to physically protect computer

resources and restrict access to sensitive information, provide appropriate segregation of duties among computer personnel, prevent unauthorized changes to operating system software, and ensure the continuation of computer processing operations in case of an unexpected interruption. Although we did not review these general controls at the Hines and Philadelphia centers, we found weaknesses in these areas at the Albuquerque, Dallas, and Austin centers.

Physical Security Controls Are Not Effective

Important general controls for protecting access to data are the physical security control measures, such as locks, guards, fences, and surveillance equipment that an organization has in place. At VA, such controls are critical to safeguarding critical financial and sensitive veteran information and computer operations from internal and external threats. We found weaknesses in physical security at each of the three facilities where these controls were reviewed.

None of the three facilities that we visited adequately controlled access to the computer room. Excessive access to the computer rooms at these facilities was allowed because none of the sites had established policies and procedures for periodically reviewing access to the computer room to determine if it was still required. In addition, the Albuquerque Medical Center was not documenting access to the computer room by individuals who required escort, such as visitors, contractors, and maintenance staff.

At the Austin Automation Center, for instance, we found that more than 500 people had access to the computer room, including more than 170 contractors. The director of the Austin Automation Center told us that since our review, access to the computer room had been reduced to 250 individuals and that new policies and procedures would be established to further scrutinize the number of staff who had access to the computer room.

In addition, both the Dallas and Albuquerque medical centers gave personnel from the information resource management group unnecessary access to the computer room. At the Albuquerque Medical Center, 18 employees from the information resource management group had access to the computer room, while at the Dallas Medical Center, all information resource management staff were allowed access. At both medical centers, this access included personal computer maintenance staff and certain administrative employees who should not require access to the computer room. While it is appropriate for information resource management staff

to have access to the computer room, care should be taken to limit access to only those employees who have a reasonable need.

Our review also identified other physical security control weaknesses. For example, windows in the Dallas Medical Center computer room were not alarmed to detect potential intruders and sensitive cabling in this computer room was not protected to prevent disruptions to computer operations. In addition, chemicals that posed a potential hazard to employees and computer operations were stored inside the computer room in Austin. Furthermore, a telecommunication panel in the Austin Automation Center computer room was also not protected, increasing the risk that network communications could be inadvertently disrupted.

The director of the Austin Automation Center told us that his staff had removed chemicals from the computer room and protected the telecommunications panel. In addition, the director of the Dallas Medical Center told us that his staff plan to address the physical security problems when the computer room is moved to a new facility.

Computer Duties Are Not Properly Segregated

Another fundamental technique for safeguarding programs and data is to segregate the duties and responsibilities of computer personnel to reduce the risk that errors or fraud will occur and go undetected. Duties that should be separated include application and system programming, quality assurance, computer operations, and data security.

At the Austin Automation Center, we found three system programmers who had been assigned to assist in the security administration function. Under normal circumstances, backup security staff should report to the security administrator and have no programming duties. Because these individuals had both system and security administrator privileges, they had the ability to eliminate any evidence of their activity in the system.

At the time of our review, Austin's security software administrator also reported to the application programming division director. The security software administrator, therefore, had application programming responsibility, which is not compatible with the duties associated with system security.

The director of the Austin Automation Center told us that actions had been taken to address the reported weaknesses. These actions included removing the master security administration user ID and password from

system programmers and establishing a new security group to consolidate security software administration. During a follow-up discussion, the director also said that an emergency ID had been established to provide system programmers with additional access when required. This approach should not only improve access controls but also provide a means to determine if system programmer access authorities need to be expanded.

We also found instances where access controls did not enforce segregation of duties principles. For example, we found nine users in the information resource management group at the Albuquerque Medical Center who had both unrestricted user access to all financial data and electronic signature key authority. These privileges would allow the users to prepare invoices and then approve them for payment without creating an audit trail.

Changes to System Software Are Not Adequately Controlled

A standard computer control practice is to ensure that only authorized and fully tested operating system software is placed in operation. To ensure that changes to the operating system software are needed, work as intended, and do not result in the loss of data and program integrity, these changes should be documented, authorized, tested, independently reviewed, and implemented by a third party. We found weaknesses in operating system software change control at the Austin Automation Center.

Although the Austin Automation Center security policy required operating system software changes to be approved and reviewed, the center had not established detailed written procedures or formal guidance for modifying operating system software. There were no formal guidelines for approving and testing operating system software changes. In addition, there were no detailed procedures for implementing these changes.

During fiscal year 1997, the Austin Automation Center made more than 100 system software changes. However, none of these changes included evidence of testing, independent review, or acceptance. In addition, the Austin Automation Center did not provide any evidence of review by technical management. Furthermore, operating system software changes were not implemented by an independent control group.

The director of the Austin Automation Center told us that his staff planned to document and implement operating system software change control procedures that require independent supervisory review and approval. In

addition, the director said that management approval will be required for each phase of the software change process.

Disaster Recovery Planning Is Not Complete

An organization must take steps to ensure that it is adequately prepared to cope with a loss of operational capability due to earthquakes, fires, accidents, sabotage, or any other disruption. An essential element in preparing for such catastrophes is an up-to-date, detailed, and fully tested disaster recovery plan. Such a plan is critical for helping to ensure that information systems can promptly restore operations and data, such as payroll processing and related records, in the event of disaster.

The disaster recovery plan for the Austin Automation Center consisted of 17 individual plans covering various segments of the organization. However, there was no overall document that integrated the 17 individual plans and set forth the roles and responsibilities of each disaster recovery team, defined the reporting lines between each team, and identified who had overall responsibility for the coordination of all 17 teams.

We also found that although the Austin Automation Center had tested its disaster recovery plan, it had only performed limited testing of network communications. This testing included the Austin Finance Center, but did not involve other types of users, such as VHA medical centers or VBA regional offices. In addition, the Austin Automation Center had not conducted unannounced tests of its disaster recovery plan, a scenario more likely to be encountered in the event of an actual disaster. Finally, a copy of the disaster recovery plan was not maintained at the off-site storage facility. In the event of a disaster, it is a good practice to keep at least one current copy of the disaster recovery plan at this location to ensure that it is not destroyed by the same events that made the primary data processing facility unavailable.

The director of the Austin Automation Center told us that he was in the process of correcting each of the deficiencies we identified. Actions he identified included (1) expanding network communication testing to include an outpatient clinic and a regional office, (2) conducting unannounced tests of the disaster recovery plan, (3) incorporating the 17 individual recovery plans into an executive plan, and (4) maintaining a copy of the disaster recovery plan at the off-site storage facility.

We found deficiencies in the disaster recovery planning at the Dallas and Albuquerque medical centers as well. At both locations (1) tests of the

disaster recovery plans had not been conducted, (2) copies of the plans were not maintained off-site, (3) backup files for programs, data, and software were not stored off-site, and (4) periodic reviews of the disaster recovery plans were not required to keep them current.

The director of the Dallas Medical Center told us that he intends to review the disaster recovery plan semiannually, develop procedures to test the plan, and identify an off-site storage facility for both the disaster recovery plan and backup files.

Computer Security Problems Are Not New at VA

The general computer control weaknesses that we identified are similar to computer security problems that have been previously identified in evaluations conducted by VA's OIG and in contractor studies.

For example, in a July 1996 report evaluating computer security at the Austin Automation Center, the OIG stated that the center's security function was fragmented, user IDs for terminated employees were still active and being used, monitoring of access activities was not being performed routinely, over 600 individuals were authorized access to the computer room, and telecommunication connections were not fully tested during disaster recovery plan testing.

Similar findings were also identified by contractors hired by the Austin Automation Center to review the effectiveness of certain aspects of its general computer controls. Specifically, Austin brought in outside contractors to evaluate security software implementation in November 1995 and network security in April 1997. The security software review determined that key operating system libraries, security software files, and sensitive programs were not adequately restricted, that more than 90 IDs did not require passwords, and that access activity was not consistently monitored. In addition, the network security review found that the center had not established a comprehensive system security policy that included network security.

The OIG also reported comparable access control and security management problems at the Hines Benefits Delivery Center in May 1997. For example, the OIG determined that access to sensitive data and programs had not been appropriately restricted and that system access activity was not reviewed regularly to identify unauthorized access attempts. The OIG also found that security efforts at the Hines Benefits

Delivery Center needed to be more focused to meet the demands of the center.

In addition, the OIG identified general computer control weaknesses at seven VA medical centers as part of a review of the IFCAP system conducted from January 1994 to November 1995. Problems identified at a majority of these medical centers were reported in March 1997. These issues included problems with restricting access to the production environment, monitoring access activity, managing user IDs and passwords, testing disaster recovery plans, and reviewing user access privileges periodically.

Furthermore, the OIG included information system security controls as a material weakness in its report on VA's consolidated financial statements for fiscal year 1997. The OIG concluded that VA assets and financial data were vulnerable to error or fraud because of significant weaknesses in computer controls. Although the Federal Managers' Financial Integrity Act (FMFIA) of 1982 requires agencies to establish controls that reasonably ensure that assets are safeguarded against waste, loss, or unauthorized use, these information system integrity weaknesses were not included in the department's FMFIA report as a material internal control weakness in fiscal year 1997.

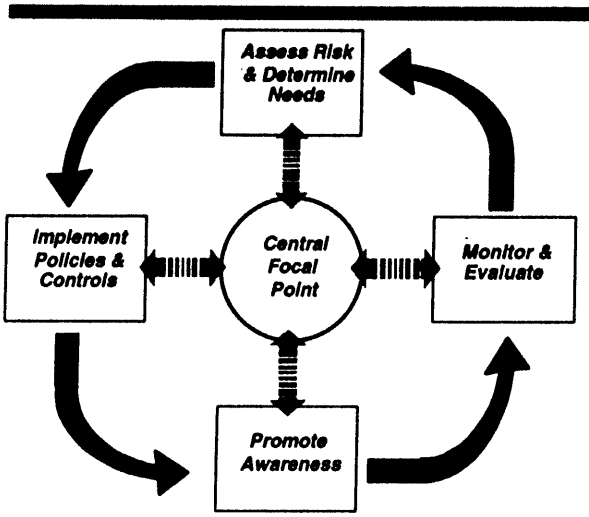
Computer Security Planning and Management Program Is Not Adequate

A key reason for VA's general computer control problems was that the department did not have a comprehensive computer security planning and management program in place to ensure that effective controls were established and maintained and that computer security received adequate attention.

To assist agencies in developing more comprehensive and effective information security programs, we studied the security management practices of eight nonfederal organizations with reputations as having superior information security programs. We found that these organizations successfully managed their information security risks through an ongoing cycle of risk management activities.[1] As shown in figure 1, each of these activities is linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

[1]For more information on the risk management cycle, see Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

Figure 1: Risk Management Cycle



The risk management cycle begins with an assessment of risks and a determination of needs. This assessment includes selecting cost-effective policies and related controls. Once policies and controls are selected, they must be implemented. Next, the policies and controls, as well as the risks that prompted their adoption, must be communicated to those responsible for complying with them. Finally, and perhaps most important, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action. In addition, our study found that a strong central security management focal point can help ensure that the major elements of the risk management cycle are carried out and can serve as a communications link among organizational units.

In contrast, VA had not instituted a framework for assessing and managing risks or monitoring the effectiveness of general computer controls. Specifically, VA's computer security efforts lacked

- clearly delineated security roles and responsibilities;
- regular, periodic assessments of risk;
- security policies and procedures that addressed all aspects of VA's interconnected environment;
- an ongoing security monitoring program to identify and investigate unauthorized, unusual, or suspicious access activity; and
- a process to measure, test, and report on the continued effectiveness of computer system, network, and process controls.

The first key problem at the locations we reviewed was that security roles and responsibilities were not clearly assigned and security management was not given adequate attention. For example, the computer security administration function at the Austin Automation Center was fragmented between computer security administration staff and other computer security components. Specifically, computer security administration staff reported to the application programming division while other computer security staff reported to a staff function within the center's management directorate. Furthermore, the computer security administration staff was responsible for application programming in addition to supporting security administration.

The director of the Austin Automation Center told us that a new security group would be formed to consolidate staff performing the security software administration and physical security functions into one group. As part of this effort, roles and responsibilities for security administration were to be explicitly assigned.

The roles and responsibilities for managing computer security at the other facilities we reviewed were also weak. For instance, computer security administration at the Philadelphia Benefits Delivery Center was limited to adding and removing users from the system, while at the Hines Benefits Delivery Center the responsibility for day-to-day security monitoring and reviewing the overall effectiveness of the security program was unclear. And at both the Dallas and Albuquerque medical centers, security administration was assigned only as a collateral responsibility. The security administrators at these medical centers reported spending less than a fifth of their time on security-related matters, which was not sufficient to actively manage and monitor access to critical medical and financial systems.

A second key aspect of computer security planning and management is periodically assessing risk. Regular risk assessments assist management in

making decisions on necessary controls by helping to ensure that security resources are effectively distributed to minimize potential loss. These assessments also increase the awareness of risks and, thus, generate support for adopted policies and controls, which helps ensure that the policies and controls operate as intended.

VA's policy requires that risk assessments be performed every 3 years or when significant changes are made to a facility or its computer systems. However, none of the three facilities where risk assessments were reviewed—Albuquerque, Dallas, and Austin—had completed risk assessments on a periodic basis or updated these assessments when significant changes occurred. For example, there was no indication that a risk assessment had ever been performed at the Albuquerque Medical Center. The Dallas Medical Center risk assessment had not been updated since 1994, even though its processing environment had changed significantly since then. The Dallas Medical Center has upgraded its computer hardware and added network capabilities since 1994. Furthermore, the Austin Automation Center did not conduct a risk assessment from 1991 through 1996, even though the center implemented a new financial management computer system during this period. The director of the Austin Automation Center told us that his staff planned to begin assessing risk on a regular basis.

A third key element of effective security planning and management is having established policies and procedures governing a complete computer security program. Such policies and procedures should integrate all security aspects of an organization's interconnected environment, including local area network, wide area network, and mainframe security. The integration of network and mainframe security is particularly important as computer systems become more and more interconnected.

VA's CIO, through the Deputy Assistant Secretary for Information Resources Management (DAS/IRM), is responsible for developing departmentwide security policies and periodically reviewing organizational compliance with the security policies. On January 30, 1997, DAS/IRM issued an updated security policy. However, this policy is still evolving and does not yet adequately establish a framework for developing and implementing effective security techniques or monitoring the effectiveness of these techniques within VA's interconnected environment. For example, the updated security policy addressed local area networks but did not provide guidance for other computer platforms, such as mainframe computer security.

A fourth key area of an overall computer security management program is an ongoing security monitoring program that helps to ensure that facilities are monitoring both successful and unsuccessful access activities. As noted above, VA did not have overall guidance on monitoring and evaluating access activities at VA processing facilities. Security administration staff at the VA facilities we visited were not actively monitoring successful or unsuccessful attempts to access sensitive computer system files. In addition, although VA has procedures for reporting computer security incidents, these procedures will not be effective until each facility establishes a mechanism for identifying computer security incidents.

A fifth key element of effective security planning and management is a process for periodically monitoring, measuring, testing, and reporting on the continued effectiveness of computer system, network, and process controls. This type of security oversight is an essential aspect of an overall security planning and management framework because it helps the organization take responsibility for its own security program and can help identify and correct problems before they become major concerns.

Although VA had taken some measures to evaluate controls periodically, the department had not established a coordinated program that provided for ongoing local oversight and periodic external evaluations. In addition, VA had not provided technical standards for implementing security software, maintaining operating system integrity, or controlling sensitive utilities. Such standards would not only help ensure that appropriate computer controls were established consistently throughout the department, but also facilitate periodic reviews of these controls.

The Austin Automation Center was the only facility we visited that had attempted to evaluate the effectiveness of its computer controls. For the last 3 years, the Austin Automation Center has brought in either OIG or contractor personnel to evaluate certain aspects of its computer security, including mainframe security software implementation, the network security environment, and physical access controls. In addition, the director of the Austin Automation Center told us that the center's client server environment and security controls would be reviewed during calendar year 1998. However, the Austin Automation Center had not established an ongoing security oversight program to ensure that controls continued to work as intended.

In addition, both the DAS/IRM security group and the VHA Medical Information Security Service (MISS) had performed security reviews, but these reviews focused on compliance rather than on the effectiveness of controls. The DAS/IRM security group evaluated disaster recovery on a departmentwide basis in fiscal year 1997; MISS reviews computer security at VHA processing facilities on a 3-year rotational basis. Despite these efforts, we found control weaknesses due to noncompliance with VA policies and procedures. Furthermore, until VA establishes a program to periodically evaluate the effectiveness of controls, it will not be able to ensure that its computer systems and data are adequately protected from unauthorized access.

In April 1998, DAS/IRM officials told us that VA is in the process of developing a comprehensive security plan and management program that will incorporate a risk management cycle and include requirements for monitoring access activity, reporting security incidents, and reviewing compliance with policies and procedures. The director of VHA MISS also told us in April 1998 that the VHA information security program office is addressing all of the security issues identified. As part of this effort, MISS plans to change its on-site security review procedures and VHA plans to expand current security policies and guidance.

Conclusions

VA's access control problems, as well as other general computer control weaknesses, are placing sensitive veteran medical and benefit information at risk of dis[illegible]are, critical financial and benefit delivery operations at risk of disruption, and assets at risk of loss. The general computer control weaknesses we identified could also adversely affect other agencies that depend on the Austin Automation Center for computer processing support.

Especially disturbing is the fact that many similar weaknesses had been reported in previous years, indicating that VA's past actions have not been effective on a departmentwide basis. Implementing more effective and lasting controls that protect sensitive veteran information and establish an effective general computer control environment requires that the department establish a comprehensive computer security planning and management program. This program should provide for periodically assessing risks, implementing effective controls for restricting access based on job requirements and proactively reviewing access activities, clearly defining security roles and responsibilities, and, perhaps most

important, monitoring and evaluating the effectiveness of controls and policies to ensure that they remain effective.

Recommendations

We recommend that you direct the VA CIO to work in conjunction with the VBA and VHA CIOs and the facility directors as appropriate to

- limit access authority to only those computer programs and data needed to perform job responsibilities and review access authority periodically to identify and correct inappropriate access;
- implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and test these controls periodically to ensure that they are operating effectively;
- develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity;
- restrict access to computer rooms based on job responsibility and periodically review this access to determine if it is still appropriate;
- separate incompatible computer responsibilities, such as system programming and security administration, and ensure that access controls enforce segregation of duties principles;
- require operating system software changes to be documented, authorized, tested, independently reviewed, and implemented by a third party; and
- establish controls to ensure that disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.

We also recommend that you develop and implement a comprehensive departmentwide computer security planning and management program. Included in this program should be procedures for ensuring that

- security roles and responsibilities are clearly assigned and security management is given adequate attention;
- risks are assessed periodically to ensure that controls are appropriate;
- security policies and procedures comprehensively address all aspects of VA's interconnected environment;
- attempts (both successful and unsuccessful) to gain access to VA computer systems and the sensitive data files and critical production programs stored on these systems are identified, reported, and reviewed on a regular basis; and

- a security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.

In addition, we recommend that you direct the VA CIO to review and assess computer control weaknesses that have been identified throughout the department and establish a process to ensure that these weaknesses are addressed.

Furthermore, we recommend that you direct the VA CIO to monitor and periodically report on the status of actions taken to improve computer security throughout the department.

Finally, we recommend that you report the information system security weaknesses we identified as material internal control weaknesses in the department's FMFIA report until these weaknesses are corrected.

Agency Comments

In commenting on a draft of this report, VA agreed with our recommendations and stated that it is taking immediate action to correct computer control weaknesses and implement oversight mechanisms to ensure that these problems do not recur. VA stated that it is also preparing a comprehensive security plan and management program that will incorporate a risk management cycle and include requirements and guidance for monitoring access activity at VA facilities.

In addition, the VA stated that its CIO is working closely with the VBA and VHA CIOs to identify computer control weaknesses previously reported in OIG reviews and other internal evaluations and develop a plan to correct these deficiencies. VA also informed us that the CIO will report periodically to the OIG on VA's progress in correcting computer control weaknesses throughout the department.

Finally, VA agreed to consider outstanding computer control weaknesses for reporting as material weaknesses in the department's fiscal year 1998 FMFIA report when the department's top management council meets in the first quarter of fiscal year 1999.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations to the Senate Committee on

Governmental Affairs and the House Committee on Government Reform and Oversight not later than 60 days after the date of this report. A written statement also must be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made more than 60 days after the date of this report.

We are sending copies of the report to the Chairmen and Ranking Minority Members of the House and Senate Committees on Veterans Affairs and to the Director of the Office of Management and Budget. Copies will also be made available to others upon request.

Please contact me at (202) 512-3317 if you or your staff have any questions. Major contributors to this report are listed in appendix II.

Sincerely yours,

Robert F. Dacey

Robert F. Dacey
Director, Consolidated Audit and
Computer Security Issues

Appendix I

Comments From the Department of Veterans Affairs

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

DEPARTMENT OF VETERANS AFFAIRS
ASSISTANT SECRETARY FOR POLICY AND PLANNING
WASHINGTON DC 20420

JUL 16 1998

Mr. Gene Dodaro
Assistant Comptroller General
Accounting and Information Management Division
U. S. General Accounting Office
441 G Street, NW
Washington, DC 20548

Dear Mr. Dodaro:

This is in response to your draft report, ***VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*** (GAO/AIMD-98-175). Your report cites numerous VA systems security breaches that concern us greatly. VA is taking immediate action to correct these deficiencies and is instituting oversight mechanisms to ensure that such a breakdown in the protection of our financial, veterans' benefit, veterans' health, and employee data systems does not recur.

See comment 1

VA fully concurs in each of the report's recommendations except for the one calling for VA to report the information system security weaknesses you identified as material internal control weaknesses reported by the Department under the Federal Managers Financial Integrity Act (FMFIA). For that recommendation, we can only concur in principle. VA's process for determining a material weakness requires a top management council to consider internal control weakness issues for reporting under FMFIA. That council will not meet until the first quarter of next fiscal year. By that time, we hope to have many of the identified internal control weaknesses corrected, thereby defusing the reporting issue. VA's assessment of progress will be the determining factor.

Enclosure (1) describes actions taken and planned to implement your recommendations. Enclosure (2) is an action plan that the Veterans Health Administration has developed to address your recommendations throughout VA's health care system. Enclosure (3) details additional actions that the Veterans Benefits Administration is taking to address your recommendations. I appreciate the opportunity to review the draft of your report.

Sincerely,

Dennis Duffy

Enclosure

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)

GAO recommends that the Secretary of Veterans Affairs direct the VA CIO to work in conjunction with the VBA and VHA CIOs and the facility directors as appropriate to

- **limit access authority to only those computer programs and data needed to perform job responsibilities and periodically review access authority to identify and correct inappropriate access;**
- **implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and periodically test these controls to ensure that they are operating effectively;**
- **develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity;**
- **restrict access to the computer room based on job responsibility and periodically review this access to determine if it is still appropriate;**
- **separate incompatible computer responsibilities such as system programming and security administration and ensure that access controls enforce segregation of duties principles;**
- **require operating system software changes to be documented, authorized, tested, independently reviewed and implemented by a third party, and**
- **establish controls to ensure disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.**

Concur - The Department's CIO is coordinating VA's response to the range of security weaknesses addressed in the above parts to the recommendation. VHA's Medical Information Security Service (MISS) is responsible for oversight of VHA's information system security program. While many of the security steps cited in this recommendation are already a part of existing policy (VHA Manual M-11, Chapter 16), some are not, and there still exists a need for oversight. MISS will incorporate compliance review procedures into its field station site visit program. VBA has established an Information Security Task Force to review the security areas that GAO identifies. The taskforce prepared a number of recommendations to correct policy shortcomings and access control concerns identified at the Hines and Philadelphia Benefits Delivery Centers.

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-96-175)
(Continued)

GAO also recommends:

that the Secretary develop and implement a comprehensive Departmentwide computer security planning and management program. Included in this program should be procedures for ensuring that

- security roles and responsibilities are clearly assigned and security management is given adequate attention;
- risks are assessed periodically to ensure that controls are appropriate;
- security policies and procedures comprehensively address all aspects of VA's interconnected environment;
- attempts (both successful and unsuccessful) to gain access to VA computer systems and sensitive data files and critical production programs stored on these systems are identified, reported and reviewed on a regular basis; and
- a security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.

Concur - VA is preparing a comprehensive security plan and management program that will include incident reporting security awareness, compliance reviews, and much more. We are also incorporating a risk management cycle into this program to enhance VA's computer control as noted in the discussion draft. In the policy we will include requirements for monitoring all access attempts as well as developing corresponding guidance in an adjoining handbook concerning evaluation access activities at all VA facilities. In addition, security awareness sessions will be conducted at our upcoming Information Technology Conference (ITC) in August, in Austin Texas.

In addition, GAO recommends that the Secretary direct the VA CIO to review and assess computer control weaknesses that have been identified throughout the department and establish a process to ensure that these weaknesses are addressed.

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)
(Continued)

Concur - VA's CIO and the two major administration CIOs are working closely with the Office of Inspector General to identify previously cited computer security weaknesses and to develop a plan with a timetable to correct those deficiencies. VA's CIO will report monthly to the OIG on progress in implementing IG's and GAO's recommendations.

Furthermore, GAO recommends that the Secretary direct the VA CIO to monitor and periodically report on the status of actions taken to improve computer security throughout the department.

Concur - VA's CIO will monitor closely the actions planned and taken to correct the computer security weaknesses throughout the Department. He will also periodically report on the progress achieved to the Inspector General.

Finally, GAO recommends that the Secretary report the information system security weaknesses GAO identified as material weaknesses in the department's FMFIA report until corrected.

See comment 1.

Concur in Principle - The Department's senior management will meet during the first quarter of Fiscal Year 1999 to identify those internal control issues that require the utmost attention to correct. At that time, they will consider the Department's information system security weaknesses for reporting as material weaknesses under the Federal Managers Financial Integrity Act. It is the Department's expectation that we will have made sufficient progress in correcting these problems to preclude such reporting.

In addition, the report should reflect the progress and changes that VA has implemented to correct problems as described in our comments to GAO's interim report. For example, the Austin Automation Center has:

a. Reassigned immediate responsibility for both data and physical security to the AAC Director.

Enclosure

DEPARTMENT OF VETERANS AFFAIRS COMMENTS
TO GAO DRAFT REPORT,
VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure
(GAO/AIMD-98-175)
(Continued)

b. Conducted an independent review to determine the appropriate methodology and technology to ensure full resolution of audit findings.

c. Prepared a detailed action plan with target dates, to specifically address all items in the audit report.

d. Assigned an AAC manager and a team of technicians to research, resolve, and document the resolution of each detailed finding in the audit report.

e. Completed resolution of most audit findings. Full resolution of the remainder is to be completed by September 30, 1998.

f. Requested the OIG and GAO to perform a follow-up review by the end of FY 1998 to verify the resolution of report findings.

Enclosure (2)

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: *VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*
Project No.: GAO/AIMD-98-175
Date of Report: June 1998

Recommendations/ Actions	Status	Completion Date

We (GAO) recommend that the Secretary of Veterans Affairs direct the VA CIO to work in conjunction with VBA and VHA CIOs and the facility directors as appropriate to:

Recommendation No. 1: Limit access authority to only those computer programs and data needed to perform job responsibilities and periodically review access authority and correct inappropriate access.

Concur

VHA's Manual M-11, Chapter 16, Paragraph 16.08 a., Procedures for System Access, addresses this specific issue. This paragraph states, "Use of VHA information assets (hardware/software/data) is restricted to those with a need for them in the performance of their duties. ..." In addition to this policy, Medical Information Security Service (MISS) is changing procedures for their site visits to include checking for compliance with this policy.

Recommendation No. 2: Implement ID and password management controls across all computer platforms to maintain individual accountability and protect password confidentiality and periodically test these controls to ensure that they are operating effectively.

Concur

VHA's Manual M-11, Chapter 1, Paragraph 16.09 f., Procedures for User Access, addresses this specific issue. It states, "Procedures should be in place to review user change of status (e.g., transfer, termination, separation)." This paragraph also lists 7 requirements dealing with this procedure. MISS will follow-up on this issue in order to

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: *VA INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

ensure that the facilities mentioned in this report have complied with the stated requirements by July 30, 1998. These requirements are included in our site visit checklist, which we utilize during our reviews for compliance at all of our facilities.

VHA Manual M-11, Chapter 14, Paragraph 16.08 also addresses this specific issue. This paragraph deals with issues of user access, password generation and the periodic changing (every 90 days) of passwords. There is no policy currently in place which requires periodic testing of these controls. MISS is currently rewriting Chapter 16 and will incorporate verbiage into this policy document to address the issue of periodic testing for these controls. The revised policy directive will be completed in draft form by August 15, 1998.

Recommendation No. 3: Develop targeted monitoring programs to routinely identify and investigate unusual or suspicious system and user access activity.

Concur

VHA Manual M-11, Chapter 14, Paragraph 16.11 d. (3) and e. (2) (g) addresses these issues. These paragraphs discuss the specific requirements for System Access/Trans-Action Logging/Audit Trials and Facility Technical Security Requirements. MISS plans to incorporate these reviews in the new facility review process by December 1, 1998.

Recommendation No. 4: Restrict access to the computer room based on job responsibility and periodically review this access to determine if it is still appropriate.

Concur

VHA Manual M-11, Chapter 14, Paragraph 16.10 b. (2) addresses this issue. It states, "All physical security requirements (e.g., key and combination hardware, security surveillance television equipment, room intrusion detectors), as identified in the risk analysis, which may be deemed necessary by the facility IRM to protect peripheral devices and microcomputers, should be compatible with and, when possible, integrated into the host site security system." Paragraph (3) states, "Access to storage media containing sensitive data shall be controlled by locks and access control

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

procedures." This is currently an active part of the on-site MISS security review process.

Recommendation No. 5: Separate incompatible computer responsibilities such as system programming and security administration and ensure that access controls enforce segregation of principle duties.

Concur

VHA Manual M-11, Chapter 16, Paragraph16.04 d., addresses this issue. It states, "...It is desirable from a security standpoint that these positions be separated so that the duties of any one person will not adversely affect the Automated Information Systems (AIS) due to conflict of interest or malicious intent." This is a standard procedure checked during the on-site MISS security review process.

Recommendation No. 6: Require operating system software changes to be documented, authorized, tested, independently reviewed and implemented by a third party.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.16, Certification and Re-certification, addresses this issue. This chapter discusses the requirements for testing of all new applications and of significant modification to existing applications. It also discusses the need to do audits or review and re-certification shall be performed at least every 3 years. Audits or reviews and re-certification are considered a part of agency vulnerability assessments and internal control reviews. MISS is currently working with a contracting firm to develop criteria and guidelines for certifying all sensitive applications and systems within VHA. A draft of this requirement is expected by October 1998. Additional requirements for this recommendation can also be found in M-11, Chapter 12, Verification.

Recommendation No. 7: Establish controls to ensure disaster recovery plans are comprehensive, current, fully tested, and maintained at the off-site storage facility.

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

Concur

VHA Manual M-11, Chapter 16, Paragraphs 16.11 c. (1) and 16.15 address this issue. These paragraphs state that each Chief, IRM Service, shall establish procedures to ensure the data required for contingency planning is current. Paragraph 16.15 deals with the overall Contingency Management process at the facility level and the procedures necessary to ensure that it is in place and working. This is a standard procedure checked during on-site MISS security review process. In addition to these procedures, the Office of the CIO also provides contingency planning software to each VHA facility as part of a national contract negotiated by the CIO.

Recommendation No. 8: Security roles and responsibilities are clearly assigned and security management is given adequate attention.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.04 a., addresses this issue. It establishes the role for an Information Security Officer (ISO) at each facility and delineates the responsibilities and programs necessary to engage a fully successful AIS security program. MISS will request that each facility employ a full-time ISO. A draft of this recommendation should be available for review by August 1, 1998.

Recommendation No. 9: Risks are assessed periodically to ensure that controls are appropriate.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.14, Procedures for Risk Analysis, addresses this issue. The assessments required by this policy are to be completed not less than every 2 years. The OCIO has provided the field with automated risk assessment software to aid in this process. MISS is currently working with a contractor to upgrade this software to a windows format and to provide computer-based training software for all users. The software is expected to be completed by July 20, 1998. System-wide availability is expected by August 20, 1998.

Action Plan in Response to OIG/GAO/MI Audits/Program Evaluations/Reviews

Name of Report: VA *INFORMATION SYSTEMS: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure*

Recommendation No. 10: Security policies and procedures comprehensively address all aspects of VA's interconnected environment.

Concur

VHA's Manual M-11, Chapter 16, Paragraph 16.11 e., Telecommunications and Networks, addresses this issue. In addition to this paragraph, VHA has also established the Internet Management Review Board, who develops policy and review compliance with independent Internet access by VHA facilities. There is currently seperately developed policy dealing with the Internet environment. This policy will be incorporated into the next version of Chapter 16. This policy will be completed in draft form by August 15, 1998.

Recommendation No. 11: Attempts (both successful and unsuccessful) to gain access to VA computer systems and sensitive data files and critical production programs stored on these systems are identified, reported and reviewed on a regular basis.

Concur

VHA Manual M-11, Chapter 16, Paragraphs 16.11 (2) and (5) address this issue. Additionally, MISS is currently working with a contractor to establish criteria for monitoring potential network security incidents and MISS is currently developing a Computer Emergency Response Capability for the VHA environment. This capability should be ready for implementation by December 1998.

Recommendation No. 12: A security oversight function, including both ongoing local oversight and periodic external evaluations, is implemented to measure, test, and report on the effectiveness of controls.

Concur

VHA Manual M-11, Chapter 16, Paragraph 16.13, Procedures for AIS Security Program Assessment, addresses this issue. This paragraph covers the need for both internal and external reviews. As stated earlier, MIS is currently working with a contractor to streamline the technical security portion of our external review process.

Enclosure (3)

Department of Veterans Affairs

Memorandum

Date: JUL 1? 1998

From: Deputy Under Secretary for Management (201)

Subj: Draft GAO Report, GAO File #2047D, EDMS #24538

To: Assistant Secretary for Policy and Planning (008)

1. VBA has begun addressing the specific concerns raised by GAO in its draft report, VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure. Our efforts include the following actions.

a. VBA established an Information Security Task Force to review the security areas identified in the GAO findings. The task force prepared a number of recommendations to correct policy shortcomings and access control concerns identified at the Hines and Philadelphia Benefits Delivery Centers.

b. VBA staff is researching the purchase of encryption software to prevent the capture of unencrypted mainframe IDs and passwords from the network.

c. Both BDCs are updating policies and operating memorandums. Hines will share its updates with Philadelphia so that both BDCs have similar procedures. These updates will address GAO concerns with respect to network controls.

d. The Philadelphia BDC has appointed a new Information Security Officer who is reviewing logs and violation reports. The Hines Security Staff is reviewing IBM Top Secret logs and is implementing the Honeywell System Security Manager software.

e. Hines and Philadelphia BDC Information Security Officers are reviewing access requirements as well as status of background investigations for VBA and contractor employees.

f. Hines BDC has prepared a Statement of Work for a full risk assessment to be conducted at the center.

Page 2

Assistant Secretary for Policy and Planning (008)

2. Our efforts to protect the privacy and security of data in our systems and the persons in our employ continue. If you desire any additional information, please contact Cheryl C. Buss, who can be reached on 202/273-6804.

Nora Egan

The following is GAO's comment on the Department of Veterans Affairs' letter dated July 16, 1998.

GAO Comment

1. Although VA only concurred in principle with our recommendation to report the information system security weaknesses we identified as material internal control weaknesses in the department's FMFIA report, the department's plans for evaluating computer control weaknesses for reporting as material weaknesses appear reasonable. VA has committed to presenting outstanding control weaknesses to the top management council when it meets in the first quarter of fiscal year 1999 to determine material FMFIA weaknesses for fiscal year 1998.

Appendix I

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Lon C. Chin, Assistant Director Edward M. Glagola, Jr., Assistant Director Shane D. Hartzler, Senior Evaluator Walter P. Opaska, Senior Evaluator Christopher J. Warweg, Senior Evaluator
Atlanta Field Office	Sharon S. Kittrell, Senior Auditor
Dallas Field Office	David W. Irvin, Assistant Director Debra M. Conner, Senior Auditor Shannon Q. Cross, Senior Evaluator Charles M. Vrabel, Senior Auditor

United States General Accounting Office

GAO

Report to the Committee on Governmental Affairs, U.S. Senate

September 1998

INFORMATION SECURITY

Serious Weaknesses Place Critical Federal Operations and Assets at Risk

GAO/AIMD-98-92

GAO **United States**
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-278910

September 23, 1998

The Honorable Fred Thompson
Chairman
The Honorable John Glenn
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

In response to your request, this report describes (1) the overall state of federal information security based on recently issued audit reports and (2) executive branch efforts over the last 2 years to improve the federal government's performance in this important area. These efforts include actions by individual agencies, the Office of Management and Budget, and the Chief Information Officers Council, as well as initiatives outlined in the recently issued Presidential Decision Directive 63 on critical infrastructure protection. Many of these improvement efforts respond to recommendations made in our September 1996 report Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110), which was also developed at your request.

If you have any questions, please call me at (202) 512-2600. This report was developed under the direction of Robert F. Dacey, Director, Consolidated Audit and Computer Security Issues, and Jack L. Brock, Jr., Director, Governmentwide and Defense Information Systems. Major contributors to this report are listed in appendix IV.

Gene L. Dodaro
Assistant Comptroller General

Executive Summary

Purpose

Due to growing concerns about our government's reliance on inadequately protected information systems to support critical and sensitive operations, the Chairman and Ranking Minority Member of the Senate Committee on Governmental Affairs asked GAO to (1) evaluate the effectiveness of federal information security practices based on the results of recent audits and (2) review efforts to centrally oversee and manage federal information security. This report describes the results of that analysis and outlines management practices that could improve the effectiveness of federal agency security programs.

Background

Federal agencies rely on computers and electronic data to perform functions that are essential to the national welfare and directly affect the lives of millions of individuals. More and more, these functions, which include national defense, tax collection, benefits payments, and law enforcement, depend on automated, often interconnected, systems and on electronic data rather than on manual processing and paper records. This shift has resulted in a number of benefits so that information can now be processed quickly and communicated almost instantaneously among federal offices, departments, and outside organizations and individuals. In addition, vast amounts of useful data are at the disposal of anyone with access to a personal computer, a modem, and telephone.

However, the government's increasing reliance on interconnected systems and electronic data also increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and services. The same factors that benefit federal operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or other malicious or mischievous 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 media such as magazines and computer bulletin boards. In addition, natural disasters and inadvertent errors by authorized computer users can have negative consequences if information resources are poorly protected.

Gauging the level of risk is difficult because summary data on computer security incidents and related damage are incomplete. However break-ins and damage of varying levels of significance have been acknowledged in

both the public and private sectors, and media reports on intrusions, fraud, and sabotage abound. In a recent survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation, 64 percent of the 520 respondents, which were from both the private and public sectors, reported computer security breaches within the last 12 months—a 16 percent increase in security breaches over those reported in a similar survey in 1997. While many of the survey respondents did not quantify their losses, those that did cited losses totaling $136 million.[1] In an October 1997 report entitled Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection described the potentially damaging implications of poor information security from a national perspective, noting that computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways that cannot yet be fully conceived.

To guard against such problems, federal agencies must take steps to understand their information security risks and implement policies and controls to reduce these risks, but previous reports indicate that agencies have not adequately met this responsibility. In September 1996, GAO reported that a broad array of federal operations were at risk due to information security weaknesses and that a common underlying cause was inadequate security program management. In that report, GAO recommended that the Office of Management and Budget (OMB) play a more proactive role in leading federal improvement efforts, in part through its role as chair of the Chief Information Officers (CIO) Council. Subsequently, in a February 1997 series of reports to the Congress, GAO designated information security as a new governmentwide high-risk area.[2] More recently, in its March 31, 1998, report on the federal government's consolidated financial statements, GAO reported that widespread computer control deficiencies also contribute to problems in federal financial management because they diminish confidence in the reliability of financial management data.[3]

Results in Brief

The expanded amount of audit evidence that has become available since mid-1996 describes widespread and serious weaknesses in the federal government's ability to adequately protect (1) federal assets from fraud

[1]"Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey," March 4, 1998.

[2]High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[3]Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998).

and misuse, (2) sensitive information from inappropriate disclosure, and (3) critical operations, including some affecting public safety, from disruption. Significant information security weaknesses were reported in each of the 24 largest federal agencies, with inadequately restricted access to sensitive data being the most widely reported problem. This and the other types of weaknesses identified place critical government operations, such as national defense, tax collection, law enforcement, and benefit payments, as well as the assets associated with these operations, at great risk of fraud, disruption, and inappropriate disclosures. In addition, many intrusions or other potentially malicious acts could be occurring but going undetected because agencies have not implemented effective controls to identify suspicious activity on their networks and computer systems.

Individual agencies have not yet done enough to effectively address these problems. Specifically, agency officials have not instituted procedures for ensuring that risks are fully understood and that controls implemented to mitigate risks are effective. Implementing such procedures as part of a proactive, organization-wide security management program is essential in today's interconnected computing environments.

Similarly, agency performance in this area is not yet being adequately managed from a governmentwide perspective, although some important steps have been taken. The CIO Council, under OMB's leadership, designated information security as a priority area in late 1997 and, since then, has taken some steps to develop a preliminary strategy, promote awareness, and identify ways to improve a federal incident response program developed by the National Institute of Standards and Technology (NIST). In May 1998, Presidential Decision Directive (PDD) 63 on critical infrastructure protection was issued. PDD 63 acknowledged computer security as a national security risk and established several entities within the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation to address critical infrastructure protection, including federal agency information infrastructures. At the close of GAO's review in August 1998, it was too early to determine how the Directive's provisions would be implemented and how they would relate to other ongoing efforts, such as those initiated by the CIO Council.

What needs to emerge is a coordinated and comprehensive strategy that incorporates the worthwhile efforts already underway and takes advantage of the expanded amount of evidence that has become available in recent years. The objectives of such a strategy should be to encourage agency improvement efforts and measure their effectiveness through an

appropriate level of oversight. This will require a more structured approach for (1) ensuring that risks are fully understood, (2) promoting use of the most cost-effective control techniques, (3) testing and evaluating the effectiveness of agency programs, and (4) acting to address identified deficiencies. This approach needs to be applied at individual departments and agencies and in a coordinated fashion across government.

Principal Findings

Significant Weaknesses at 24 Major Agencies Place Critical Operations at Risk

Audit reports issued from March 1996 through August 1998 identified significant information security weaknesses in each of the 24 agencies covered by the analysis. The most widely reported type of weakness was poor control over access to sensitive data and systems. This type of weakness makes it possible for an individual or group to inappropriately modify or destroy sensitive data or computer programs or inappropriately obtain or disclose confidential information for malicious purposes, such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with minimal computer and telecommunications resources and expertise.

These weaknesses place a broad range of critical operations and assets at great risk of fraud, misuse, and disruption. For example, weaknesses at the Department of Defense increase the vulnerability of various military operations that support the Department's warfighting capability, and weaknesses at the Department of the Treasury increase the risk of fraud associated with billions of dollars of federal payments and collections.

In addition, information security weaknesses place an enormous amount of highly sensitive data at risk of inappropriate disclosure. For example, weaknesses at agencies such as the Internal Revenue Service, the Health Care Financing Administration, the Social Security Administration, and the Department of Veterans Affairs place sensitive tax, medical, and other personal records at risk of disclosure.

As significant as these reported weaknesses are, it is likely that the full extent of control problems at individual agencies has not yet surfaced

because key areas of controls at many agencies have not been assessed. In particular, agency managers, who are primarily responsible for ensuring adequate security, have not fully evaluated the adequacy of their computer-based controls. In addition, audits at most agencies have not yet fully covered controls associated with operating system software, which are critical to the security of all of the applications the systems support. In agencies where this control area was reviewed, weaknesses were always identified.

Improved Security Program Planning and Management Needed at Individual Agencies

Poor security program planning and management continue to be fundamental problems. Agencies have not yet developed effective procedures for assessing computer security risks, determining which risks are significant, assigning responsibility for taking steps to reduce risks, and ensuring that these steps remain effective. Security planning and management deficiencies were reported for 17 of the 24 agencies included in GAO's analysis and numerous recommendations have been made to address specific agency deficiencies.

To identify potential solutions to this problem, GAO studied the security management practices of eight organizations known for their superior security programs. These organizations included two financial institutions, a retailer, an equipment manufacturing company, a state university, a state agency, a regional electric utility, and a computer vendor. GAO found that these organizations managed their information security risks through a cycle of risk management activities, and it identified 16 specific practices that supported these risk management principles.

These practices involve (1) establishing a central security management focal point, (2) assessing risk, (3) selecting and implementing cost-effective policies and controls, (4) promoting awareness, and (5) continually evaluating and improving control effectiveness. They also emphasize the importance of viewing information security program management as an integral component of managing agency operations and of involving both program managers and technical experts in the process.

GAO published the findings from this study in the May 1998 executive guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), which has been endorsed by the Federal CIO Council. The guide's findings are summarized in chapter 3 of this report.

The security management practices described in GAO's executive guide are most likely to be successful if they are implemented as part of broader improvements to information technology management. Such improvements are underway across government due to specific information technology management reforms mandated by the Paperwork Reduction Act amendments of 1995 and the Clinger-Cohen Act of 1996.

Initiatives to Improve Central Coordination and Management Need to Provide a Comprehensive Strategy

Individual agencies are primarily responsible for the security of their information resources, but central management also is important to (1) ensure that federal executives understand risks to their operations, (2) monitor agency performance in mitigating these risks, (3) facilitate implementation of any needed improvements, and (4) address issues that affect multiple agencies. Under the Paperwork Reduction Act, this oversight responsibility lies with OMB.

Since September 1996 when GAO reported that OMB needed to strengthen its oversight of agency practices, the CIO Council, under OMB's leadership, has become a component of the administration's efforts to address federal information security problems and has taken some actions in this regard. Specifically, during 1997, the Council designated information security as one of six priority areas and, late in the year, established a Security Committee. Since then, the Committee has (1) developed a preliminary plan for addressing various aspects of the problem, (2) established links with other federal entities involved in security issues, (3) held a security awareness day for federal CIOs, deputy CIOs, and security officers, and (4) developed plans for reorienting the Federal Computer Incident Response Capability (FedCIRC), a program initiated by NIST to assist agencies in improving their security incident response capabilities and other aspects of their security programs.

In addition, OMB has continued to monitor selected agency system-related projects, many of which have significant security implications. However, neither OMB nor the CIO Council has yet developed a program for comprehensively overseeing and managing the security of critical federal operations by ensuring that agency programs are adequately evaluated and that the results are used to measure and prompt improvements, as recommended in GAO's September 1996 report.

Concurrent with OMB and CIO Council efforts during late 1997 and early 1998, the administration developed and issued PDD 63 in response to recommendations made by the President's Commission on Critical

Infrastructure Protection. The Directive acknowledges computer security risk as a national security risk, addresses a range of national infrastructure protection issues, and includes several provisions intended to ensure that critical federal computer, or "cyber-based," systems are protected from attacks by our nation's enemies. Also, it establishes a National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, who reports to the President through the Assistant to the President for National Security Affairs; a Critical Infrastructure Coordination Group; and a Critical Infrastructure Assurance Office within the Department of Commerce. The Directive outlines planned actions pertaining to federal information security, which include:

- requiring each federal department and agency to develop a plan for protecting its own critical infrastructure, including its cyber-based systems;
- reviewing existing federal, state, and local entities charged with information assurance tasks;
- enhancing collection and analysis of information on the foreign information warfare threat to our critical infrastructures;
- establishing a National Infrastructure Protection Center within the Federal Bureau of Investigation to facilitate and coordinate the federal government's investigation and response to attacks on its critical infrastructures;
- assessing U.S. Government systems' vulnerability to interception and exploitation; and
- incorporating agency infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

Though some of these efforts have begun, at this early stage of implementation, it is unclear how the provisions outlined in the Directive will be implemented and how they will be coordinated with other related efforts, such as those of the CIO Council.

Conclusion

Since September 1996, the need for improved federal information security has received increased visibility and attention. Important efforts have been initiated to address this issue, but more effective actions are needed both at the individual agency level and at the governmentwide level. Many aspects of the recommendations GAO made in September 1996 are still applicable. In particular, a comprehensive governmentwide strategy needs to be produced. The CIO Council's efforts during late 1997 and the first half of 1998, as well as issuance of PDD 63 in May 1998, indicate that senior

federal officials are increasingly concerned about information security risks, both to federal operations as well as to privately controlled national infrastructures, and are now moving to address these concerns. Coordinated efforts throughout the federal community, as envisioned by PDD 63, will be needed to successfully accomplish the objectives of these efforts and substantively improve federal information security. It is especially important that a governmentwide strategy be developed that clearly defines and coordinates the roles of new and existing federal entities in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation and support.

Recommendation

GAO recommends that the Director of OMB and the Assistant to the President for National Security Affairs ensure that the various existing and newly initiated efforts to improve federal information security are coordinated under a comprehensive strategy. Such a strategy should

- ensure that executive agencies are carrying out the responsibilities outlined in laws and regulations requiring them to protect the security of their information resources;
- clearly delineate the roles of the various federal organizations with responsibilities related to information security;
- identify and rank the most significant information security issues facing federal agencies;
- promote information security risk awareness among senior agency officials whose critical operations rely on automated systems;
- identify and promote proven security tools, techniques, and management best practices;
- ensure the adequacy of information technology workforce skills;
- ensure that the security of both financial and nonfinancial systems is adequately evaluated on a regular basis;
- include long-term goals and objectives, including time frames, priorities, and annual performance goals; and
- provide for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

Agency Comments and Our Evaluation

In commenting on a draft of this report, OMB's Acting Deputy Director for Management stated that OMB and the CIO Council, working with the National Security Council, have developed a plan to address the PDD 63 provision that the federal government serve as a model for critical infrastructure protection and to coordinate the new requirements of the

PDD with the existing requirements of the various laws pertaining to federal information security. The comments further stated that the plan is to develop and promote a process by which government agencies can (1) identify and assess their existing security posture, (2) implement security best practices, and (3) set in motion a process of continued maintenance. Also described are plans for a CIO Council-sponsored interagency security assist team that will review agency security programs. Regarding our conclusion that many aspects of the recommendations in our September 1996 report are still applicable, OMB reiterated its concern that the 1996 report's "overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security." The full text of OMB's comments is reprinted in appendix III.

OMB's comments indicate that it, the CIO Council, and the National Security Council are moving to coordinate their responsibilities and beginning to develop the comprehensive strategy that is needed. Based on the description provided, the plans being developed include several key elements, most notably a means of evaluating agency performance. These plans were still being finalized at the close of our work and were not yet available for our review. Accordingly, we are not able to comment on their content, scope, and detail, or whether they will be effective in improving federal information security.

Regarding OMB's concern that we have overemphasized its role, we agree that agency managers are primarily responsible for the security of their operations. Increased attention and support from central oversight, if done effectively, should not distract agencies from their responsibilities in this area. On the contrary, active oversight of agency performance is more likely to have the effect of emphasizing the agency managers' accountability and providing more visibility for agencies that are achieving their information assurance goals as well as those that are falling short.

Contents

Table

Figure

Abbreviations

CFO	Chief Financial Officer
CIO	Chief Information Officer
DOD	Department of Defense
FAA	Federal Aviation Administration
FedCIRC	Federal Computer Incident Response Capability
FMFIA	Federal Managers' Financial Integrity Act
IG	Inspector General
GAO	General Accounting Office
HCFA	Health Care Financing Administration
HHS	Department of Health and Human Services
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PDD	Presidential Decision Directive
SSA	Social Security Administration
VA	Department of Veterans Affairs

Chapter 1

Introduction

This report provides a summary analysis of recently reported information security weaknesses at federal agencies and describes management practices that federal agencies can adopt to help improve their security programs. It also describes centralized efforts to oversee and manage federal information security from a governmentwide perspective.

The vulnerabilities associated with our nation's reliance on interconnected computer systems are a growing concern. At the federal level, such systems process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations. Because of the importance of establishing and maintaining adequate security over federal operations, Senators Fred Thompson and John Glenn, Chairman and Ranking Minority Member, respectively, of the Senate Committee on Governmental Affairs, have undertaken an effort to address the various management, technical, and operational aspects of this problem. As part of that effort, they requested that we (1) summarize the effectiveness of federal information security, based on recently issued audit reports, (2) describe actions agencies can take to improve their security programs, and (3) evaluate actions taken by the Office of Management and Budget (OMB) and the federal Chief Information Officers (CIO) Council to address federal information security problems. This resulting report is one of several reviews that Chairman Thompson and Senator Glenn have requested as part of their ongoing oversight of federal information security and other aspects of information technology management. Related GAO reports are listed in appendix I.

Computers and Electronic Data Are Indispensable to Federal Operations

Federal agencies perform important functions that are essential to the national welfare and directly affect the lives of millions of individuals everyday. More and more, these functions, which include national defense, tax collection, import control, benefits payments, and law enforcement, depend on automated, often interconnected, systems and on electronic data rather than on manual processing and paper records. The benefits of this shift are increasingly obvious—information can be processed quickly and communicated almost instantaneously among federal offices, departments, and outside organizations and individuals. In addition, vast amounts of data are at the disposal of anyone with access to a personal computer, a modem, and telephone.

However, the government's increasing reliance on interconnected systems and electronic data also increases the risks of fraud, inappropriate disclosure of sensitive data, and disruption of critical operations and

services. The same factors that benefit federal operations—speed and accessibility—also make it possible for individuals and organizations to inexpensively interfere with or eavesdrop on these operations from remote locations for purposes of fraud or sabotage, or other malicious or mischievous 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.

Gauging the risk is difficult because summary data on computer security incidents and related damage are incomplete. However, in an October 1997 report entitled Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection described the potentially devastating implications of poor information security from a national perspective, noting that computerized interaction within and among infrastructures has become so complex that it may be possible to do harm in ways we cannot yet conceive. According to a recent statement by the Director of the National Security Agency, attacks on public and private systems occur everyday. For example, in February 1998, hackers used tools and techniques readily available on Internet bulletin boards to attack systems at the Department of Defense. Media reports on intrusions, fraud, and sabotage abound, and, in a recent survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation, 64 percent of the 520 respondents from the private and public sector reported computer security breaches within the last 12 months. This is a 16-percent increase in security breaches over those reported in a similar survey in 1997 and a 22-percent increase over those reported in 1996.[1]

To guard against such problems, federal agencies, like other computer-dependent organizations, must take steps to understand their information security risks and implement policies and controls to reduce these risks. Specifically, federal agencies must protect the integrity and, in some cases, the confidentiality of the enormous amounts of sensitive data they maintain, such as personal information on individuals, financial transactions, defense inventories, operational plans, and regulatory inspection records. In addition, they must take steps to ensure that

[1]"Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey," March 4, 1998.

computerized operations supporting critical government functions are not severely disrupted.

Previous Reports Have Identified Significant Security Problems

Although the government's reliance on computers and telecommunications has been rapidly growing, reports over the last few years indicate that federal operations and data are inadequately protected and that these problems are serious and pervasive. In September 1996, we reported that, since September 1994, serious weaknesses had been reported for 10 of the largest 15 federal agencies.[2] In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences, and we recommended that OMB play a more proactive role in overseeing agency practices and managing improvements, in part through its role as chair of the CIO Council. Subsequently, in February 1997, in a series of reports to the Congress, we designated information security as a new governmentwide high-risk area.[3] Most recently, in our March 31, 1998, report on the federal government's consolidated financial statements, we reported that widespread and serious computer control weaknesses affect virtually all federal agencies and significantly contribute to many material deficiencies in federal financial management.[4] In that report, we also noted that these weaknesses place enormous amounts of federal assets at risk of fraud and misuse, financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption.

During 1996 and 1997, federal information security was also addressed by the President's Commission on Critical Infrastructure Protection, which had been established to investigate our nation's vulnerability to both "cyber" and physical threats. In its October 1997 report, Critical Foundations: Protecting America's Infrastructures, the Commission described the potentially devastating implications of poor information security from a national perspective. The report also recognized that the federal government must "lead by example," and included recommendations for improving government systems security, expediting efforts to facilitate the use of encryption, developing risk assessment

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

[3]High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

[4]Financial Audit: 1997 Consolidated Financial Statements of the United States Government (GAO/AIMD-98-127, March 31, 1998).

methods, measuring performance, and elevating threat assessments as a foreign intelligence priority.

A number of factors contribute to poor federal information security including insufficient awareness and understanding of risks, a shortage of staff with needed technical expertise, a lack of systems and security architectures to facilitate implementation and management of security controls, and various problems associated with the availability and use of specific technical controls and monitoring tools. All of these are important; however, an underlying theme that was identified in our September 1996 report is a lack of security program management and oversight to ensure that risks are identified and addressed and that controls are working as intended.

Responsibilities Outlined in Laws and Guidance

The need to protect sensitive federal data maintained on automated systems has been recognized for years in various laws and in federal guidance. The Privacy Act of 1974, as amended; the Paperwork Reduction Act of 1980, as amended; and the Computer Security Act of 1987 all contain provisions requiring agencies to protect the confidentiality and integrity of the sensitive information that they maintain. The Computer Security Act (Public Law 100-235) defines sensitive information as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy."

In accordance with the Paperwork Reduction Act of 1980 (Public Law 96-511), OMB is responsible for developing information security policies and overseeing agency practices. In this regard, OMB has provided guidance for agencies in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Since 1985, this circular has directed agencies to implement an adequate level of security for all automated information systems that ensures (1) effective and accurate operations and (2) continuity of operations for systems that support critical agency functions. The circular establishes a minimum set of controls to be included in federal agency information system security programs and requires agencies to periodically review system security. Responsibility for developing technical standards and providing related guidance for

sensitive data belongs primarily to the National Institute of Standards and Technology (NIST), under the Computer Security Act.

The Clinger-Cohen Act of 1996 recently reemphasized OMB, NIST, and agency responsibilities regarding information security under a broader set of requirements aimed at improving information technology management in general. In particular, the act stipulated that agency heads are directly responsible for information technology management, including ensuring that the information security policies, procedures, and practices of their agencies are adequate. The act also required the appointment of a CIO for each of the 24 largest federal agencies to provide the expertise needed to implement needed reforms. Subsequently, in July 1996, the President established the CIO Council, chaired by OMB, to address governmentwide technology issues and advise OMB on policies and standards needed to implement legislative reforms. Council members include CIOs and Deputy CIOs from each of the major agencies.

The adequacy of controls over computerized data and the management of these controls are also addressed indirectly by the following additional laws:

- The Federal Managers' Financial Integrity Act (FMFIA) of 1982 requires agency managers to annually evaluate their internal control systems and report to the President and the Congress any material weaknesses that could lead to fraud, waste, and abuse in government operations.
- The Chief Financial Officers (CFO) Act of 1990, as expanded by the Government Management Reform Act of 1994, requires agency CFOs to develop and maintain financial management systems that provide complete, reliable, consistent, and timely information. Under the act, major federal agencies prepare annual financial statements and have them audited by their respective inspectors general. In practice, such audits generally include evaluating and testing controls over the security of automated financial management systems.
- The Federal Financial Management Improvement Act of 1996 requires auditors to report whether agency financial management systems comply with certain established financial management systems requirements. OMB guidance to agency CFOs and IGs lists these systems requirements, which include security over financial systems provided in accordance with OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Agency managers are responsible for developing remediation plans to address the problems noted by the auditors.

- The Government Performance and Results Act of 1993 requires agencies to establish goals for program performance, measure results, and report annually on program performance to the President and the Congress.

In May 1998, Presidential Decision Directives 62 and 63 established additional requirements for ensuring protection of our nation's critical infrastructures from both physical and "cyber," or computer-based, threats. At the close of our fieldwork in August 1998, it was too early to determine how these directives would be implemented. However, the provisions pertaining to federal agency information security that are specified in Directive 63 are summarized in chapter 4. Presidential Decision Directive 62, which pertains to counter-terrorism responsibilities, is classified and, therefore, is not discussed in this report.

Objectives, Scope, and Methodology

The objectives of this report are to

- describe the extent of federal information security problems and the associated risks based on reports issued since March 1996,
- identify management actions that could effect significant and long-term improvements in information security at the individual agency level, and
- evaluate governmentwide efforts to improve information security, especially actions taken since September 1996 by OMB and the CIO Council, and identify needed additional actions.

To describe the extent of information security problems and associated risks, we analyzed findings from over 80 GAO and agency reports, including inspector general (IG) reports, issued from March 1996 through September 1998. These included some reports for which distribution has been restricted because they discuss sensitive aspects of agency operations. Although we considered the results of these restricted reports when developing summary data on agency weaknesses, the related findings are not discussed in detail nor the agency identified. The reports we considered pertained to the 24 federal departments and agencies covered by the CFO Act. Together these departments and agencies accounted for about 99 percent of the total reported federal net outlays in fiscal year 1997. The reports we analyzed, excluding those that are restricted, are listed in appendixes I and II.

In analyzing reported findings, we categorized them into six basic areas of general control: security program planning and management, access control, application program change control, segregation of duties,

operating systems security, and service continuity. These six areas of general controls provide a framework for comprehensively evaluating information security. The six categories are defined and described in chapter 2.

To identify management actions that could effect fundamental improvements in security at individual agencies, we summarized the results of our recent study of information security program management practices at leading organizations. We performed this study because previous audits had shown that poor security program management was an underlying cause of information security control weaknesses. In May 1998, we published the results of this study as an executive guide entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68).

To assess OMB's leadership and coordination of federal information security efforts, we met with officials from OMB's Office of Information and Regulatory Affairs to discuss their activities related to information security and progress on recommendations made in our report Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110, September 24, 1996). We also discussed the information security-related activities of the federal CIO Council with members of the Council's Security Committee and reviewed related documentation, such as meeting minutes and the CIO Council's January 1998 governmentwide strategic plan for information resources management.

We also obtained and reviewed Presidential Decision Directive 63, which was issued May 22, 1998, late in our review. This directive specifies requirements for protecting our nation's critical infrastructures and includes provisions pertaining to federal agency information security.

Our review was conducted from December 1997 through August 1998 in accordance with generally accepted government auditing standards. One of the reports we relied on, VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse, and Improper Disclosure (GAO/AIMD-98-175), is being issued in September 1998. However, a complete draft was available at the close of our review in August. OMB provided written comments on a draft of this report, which are discussed in the "Agency Comments and Our Evaluation" section in chapter 4 and reprinted in appendix III.

Related GAO Efforts

In addition to this report, we have worked with the Congress, primarily the Senate Committee on Governmental Affairs, to pursue a comprehensive strategy for addressing the federal information security problems. This strategy involves supplementing our audit work with research projects and other actions to promote and provide support for federal efforts in this area. This strategy comprises the following activities:

- To assess the effectiveness of federal information security and assist the Congress in its oversight role, we are continuing to perform audits at selected individual agencies and develop specific recommendations for improvement. Some of these evaluations are performed as part of our financial statement audits at individual agencies and some pertain to nonfinancial mission-critical systems.
- To assist agency inspectors general in conducting or arranging for information security audits, we began an extensive effort during 1997 to evaluate such audit efforts at each of 24 major federal agencies. We performed, and will continue to perform, this work in conjunction with our annual audits of the consolidated financial statements of the federal government, which are required under the CFO Act as expanded by the Government Management Reform Act. At many of these agencies, we have provided extensive on-site guidance to the inspector general staff to ensure that we could rely on their audit conclusions.
- To promote more comprehensive audits of federal information security, in August 1997, we issued an exposure draft of our Federal Information System Controls Audit Manual (GAO/AIMD-12.19.6), which describes a methodology for evaluating federal agency information security programs. This methodology has guided our own audit work for several years and has recently been adopted by many agency inspectors general.
- To assist in improving the expertise of federal audit staff, we have engaged contractors and partnered with organizations, such as the Information Systems Audit and Control Association, to offer technical training sessions for GAO and IG staff involved in evaluating computer-based controls.
- To promote a broader understanding among federal managers of the practices that make an information security program successful, during 1997, we studied the practices of eight nonfederal organizations and developed an executive guide that summarizes the results. This guide, entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68) was published in May 1998. We are now working with agencies, including OMB, and the CIO Council to encourage agencies to implement these practices.
- To promote more effective central leadership, oversight, and coordination, we are continuing to monitor and work with OMB, the CIO Council, NIST, and

others with a governmentwide role regarding information security, including entities established under Presidential Decision Directive 63 to protect our nation's critical infrastructures.

- To assist the Congress, we are continuing to provide status reports on information security as a high-risk issue and information on related topics, as requested.

Chapter 2

Significant Weaknesses Identified at All Major Agencies

Evaluations of computer security published since March 1996 present a disturbing picture of the federal government's lack of success in protecting its assets from fraud and misuse, sensitive information from inappropriate disclosure, and critical operations from disruption. Significant information security weakness were identified in each of the 24 agencies covered by our analysis—agencies that in fiscal year 1997 accounted for 99 percent of reported federal net outlays. These weaknesses place a broad range of critical operations and assets at risk for fraud, misuse, and disruption. In addition, they place an enormous amount of highly sensitive data, much of it on individual taxpayers and beneficiaries, at risk of inappropriate disclosure.

Weaknesses were reported in a variety of areas that we have categorized into six areas of "general controls." General controls are the policies, procedures, and technical controls that apply to all or a large segment of an entity's information systems and help ensure their proper operation. The most widely reported weakness was poor control over access to sensitive data and systems. This type of weakness makes it possible for an individual or group to inappropriately modify, destroy, or disclose sensitive data or computer programs for purposes such as personal gain or sabotage. In today's increasingly interconnected computing environment, poor access controls can expose an agency's information and operations to attacks from remote locations all over the world by individuals with minimal computer and telecommunications resources and expertise.

The full extent of control problems is not known because all six of the general control areas were reviewed at only 9 of the 24 agencies. In particular, most audits have not yet covered controls associated with system software, which are critical to the security of all applications supported by a system. In agencies where this control area was reviewed, weaknesses were always found, as shown in table 1.

Table 1 provides an overview of the types of weaknesses reported throughout the government, as well as the gaps in audit coverage. The pages following Table 1 describe (1) the risks these weaknesses pose to major federal operations and (2) common types of deficiencies identified in each of the six general control categories.

Table 2.1: Areas of Information Security Weakness Reported for the 24 Largest Agencies

General control area	Number of agencies: Significant weakness identified	No significant weakness identified	Area not reviewed
Entitywide security program planning and management	17	0	7
Access controls	23	0	1
Application software development and change controls	14	4	6
Segregation of duties	16	1	7
System software controls	9	0	15
Service continuity controls	20	0	4

Note: Most of the audits used to develop this table were performed as part of financial statement audits. At some agencies with primarily financial-related missions, such as the Department of the Treasury and the Social Security Administration, these audits covered the bulk of mission-related operations. However, at other agencies whose missions are primarily nonfinancial, such as the Departments of Defense and Justice, the audits used to develop this table may provide a less complete picture of the agency's overall security posture because the audit objectives focused on the financial statements and did not include evaluating systems supporting nonfinancial operations. Nevertheless, at agencies where computer-based controls over nonfinancial operations have been audited, similar weaknesses have been identified.

Examples of Weaknesses at Individual Agencies Highlight Risks

To understand the significance of the weaknesses summarized in table 1, it is necessary to link them to the risks they present to federal operations and assets. Virtually all federal operations are supported by automated systems and electronic data, and agencies would find it difficult, if not impossible, to carry out their missions and account for their resources without these information assets. Descriptions of reported weaknesses and related risks to selected major federal operations follow.

Department of the Treasury

The Department of the Treasury, which includes the Internal Revenue Service; U.S. Customs Service; Bureau of the Public Debt; Financial Management Service; and Bureau of Alcohol, Tobacco, and Firearms; relies on computer systems to process, collect or disburse, and account for over a trillion dollars in federal receipts and payments annually. In addition, the department's computers handle enormous amounts of highly sensitive data associated with taxpayer records and law enforcement operations and support operations critical to financing the federal government, maintaining the flow of benefits to individuals and organizations, and controlling imports and exports.

Protecting these operations and assets is essential to the welfare of our nation. However, weaknesses have been reported for several of Treasury's major bureaus, and, in some cases, these weaknesses have been outstanding for years. For example:

- In March 1998, the Treasury IG reported that deficiencies in the effectiveness of computer-based controls in multiple bureaus constituted a material weakness in the department's internal control structure and increased the risk that unauthorized individuals could intentionally or inadvertently add, alter, or delete sensitive data and programs.[1]
- In three 1997 reports,[2] we identified a wide range of continuing serious weaknesses in IRS systems, including inadequate controls over employee browsing of taxpayer records, an area that has received considerable attention for several years and was recently addressed by legislation specifying penalties for such browsing.[3]
- In March 1998, the Treasury IG reported Customs Service weaknesses associated with systems supporting trade, financial management, and law enforcement functions. Many of these weaknesses had been reported annually since 1994.[4]

Numerous recommendations have been made to Treasury bureaus over the years to correct these weaknesses, and many corrective actions are underway. In particular, IRS recently began a broad effort to strengthen its overall security program by centralizing responsibility for security issues within a newly created executive-level office and increasing investments in physical security. Further, the Financial Management Service concurred with our recommendations and is developing corrective action plans.

Department of Defense

The Department of Defense (DOD) relies on a vast and complex information infrastructure to support critical operations such as designing weapons, identifying and tracking enemy targets, paying soldiers, mobilizing reservists, and managing supplies. Indeed, its very warfighting

[1]Report on the Department of the Treasury's Fiscal Year 1997 Custodial Schedules and Administrative Statements (OIG-98-066, March 30, 1998), as included in the Department of the Treasury's Accountability Report for Fiscal Year 1997.

[2]IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997); Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-88, August 29, 1997); Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

[3]Taxpayer Browsing Protection Act (Public Law 105-35).

[4]Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1997 and 1996 Financial Statements (OIG-98-060, March 6, 1998).

capability is dependent on computer-based telecommunications networks and information systems. Defense's computer systems are particularly susceptible to attack through connections on the Internet, which Defense uses to enhance communication and information sharing.

In May 1996, we reported that attacks on Defense computer systems were a serious and growing threat.[5] The exact number of attacks could not be readily determined because tests showed that only a small portion were actually detected and reported. However, the Defense Information Systems Agency estimated that attacks numbered in the hundreds of thousands per year, were successful 65 percent of the time, and that the number of attacks was doubling each year. At a minimum, these attacks are a multimillion dollar nuisance to Defense. At worst, they are a serious threat to national security. According to Defense officials, attackers have obtained and corrupted sensitive information—they have stolen, modified, and destroyed both data and software. They have installed unwanted files and "back doors" which circumvent normal system protection and allow attackers unauthorized access in the future. They have shut down and crashed entire systems and networks, denying service to users who depend on automated systems to help meet critical missions. Numerous Defense functions have been adversely affected, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll. In March 1998, DOD announced that it had recently identified a series of organized intrusions, indicating that such events continue to be a problem.

The same weaknesses that allow attacks from outsiders could also be exploited by authorized users to commit fraud or other improper or malicious acts. In fact, a knowledgeable insider with malicious intentions can be a more serious threat to many operations since he or she is more likely to know of system weaknesses and how to disguise inappropriate actions.

Subsequent reports have identified a broad array of specific control weaknesses that increase the risks of damage from such attacks, as well as from malicious acts and inadvertent mistakes by authorized users. For example, in September 1997, we reported that Defense had not adequately (1) controlled the ability of computer programmers to make changes to systems supporting the Military Retirement Trust Fund, (2) controlled access to sensitive information on pension fund participants, or

[5]Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

(3) developed or tested a comprehensive disaster recovery plan for the sites that process Fund data. These weaknesses expose sensitive data maintained by these systems to unnecessary risk of disclosure and, should a disaster occur, there is no assurance that the operations supported by these facilities could be restored in a timely manner.[6] Similarly, In October 1997, the Defense IG reported serious authentication and access control weaknesses associated with a system that, in fiscal year 1996, maintained contract administration and payment data associated with a reported 387,000 contracts for which the reported value was over $810 billion.[7] Weaknesses in other areas, too sensitive to be reported publicly, pose risks of more serious consequences.

Reports to DOD have included numerous recommendations related to specific control weaknesses as well as the need for improved security program management. DOD is taking a variety of steps to address these problems and is establishing the Departmentwide Information Assurance Program to improve and better coordinate the information security-related activities of the military services and other DOD components.

Department of Health and Human Services

In August 1997 and April 1998, the Health and Human Services (HHS) IG reported serious control weaknesses affecting the reliability, confidentiality, and availability of data throughout the department.[8] Most significant were weaknesses associated with the Department's Health Care Financing Administration (HCFA), which, according to its reports, was responsible for processing health care claims for over 38 million beneficiaries and expending 84 percent of HHS' $340 billion fiscal year 1997 budget. HCFA relies on extensive data processing operations at its central office and about 60 contractors using multiple shared systems to collect, analyze and process personal health, financial, and medical data associated with about 853 million Medicare claims, annually.

In the 1997 report, the IG reported that Medicare contractors were not adequately protecting confidential personal and medical information associated with claims submitted. As a result, contractor employees could potentially browse data on individuals, search out information on

[6]Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

[7]General and Application Controls Over the Mechanization of Contract Administration Services System, DODIG, Report Number 98-007, October 9, 1997.

[8]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-0001, August 29, 1997) and Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1997 (A-17-98-0001, April 1, 1998).

acquaintances or others, and, possibly, sell or otherwise use this information for personal gain or malicious purposes. Similar conditions were reported in 1998.

In the 1998 report, the IG reported that data security remained a major concern at HCFA's central office. Auditor's tests showed that although HCFA corrected weaknesses found in the prior year, it was possible to gain access to the mainframe database and modify managed care production files. In addition, the IG found that users without specific authorization could potentially gain update access to those same files. Further, as reported in 1997 and 1998, because controls over operating system software were ineffective, knowledgeable individuals could surreptitiously modify or disable security controls without detection.

In both its 1997 and 1998 reports, the IG recommended that (1) systems access be properly controlled, passwords be granted consistent with assigned responsibilities, and passwords be periodically changed, (2) application development and program change control procedures be in place to protect against unauthorized changes, (3) computer-related duties be properly segregated, and (4) service continuity plans be kept current and periodically tested. HHS has recognized the need to protect the security of information technology systems and the data contained in them. Starting in 1997, HHS began to revise security policies and guidance and required each major operating division to develop and implement corrective action plans to address each major weakness identified in the August 1997 report.

Social Security Administration

The Social Security Administration (SSA) relies on extensive information processing resources to carry out its operations, which, for 1997, included payments that totaled $390 billion to 50 million beneficiaries. This represents about 25 percent of the $1.6 trillion in that year's federal expenditures. The administration also issues social security numbers and maintains earnings records and other personal information on virtually all U. S. citizens. According to SSA, no other public program or public-service entity directly touches the lives of so many people.

The public depends on SSA to protect trust fund revenues and assets from fraud and to protect sensitive information on individuals from inappropriate disclosure. In addition, many current beneficiaries rely on the uninterrupted flow of monthly payments to meet their basic needs. However, in November 1997, the Social Security Administration IG

reported widespread weaknesses in controls over access, continuity of service, and software program changes that unnecessarily place these assets and operations at risk.[9]

Access control weaknesses exposed the agency and its computer systems to external and internal intrusion, thus subjecting sensitive SSA information to potential unauthorized access, modification, or disclosure. Other weaknesses increased risks of introducing errors or irregularities into data processing operations and allowed some individuals to bypass critical controls, such as authorization and supervisory review.

Such weaknesses increase the risk that an individual or group could fraudulently obtain payments by creating fictitious beneficiaries or increasing payment amounts. Similarly, such individuals could secretly obtain sensitive information and sell or otherwise use it for personal gain. The recent growth in "identity theft," where personal information is stolen and used fraudulently by impersonators for purposes such as obtaining and using credit cards, has created a market for such information. According to the SSA IG's September 30, 1997, report to the Congress (included in the SSA's fiscal year 1997 Accountability Report), 29 criminal convictions involving SSA employees were obtained during fiscal year 1997, most of which involved creating fictitious identities, fraudulently selling SSA cards, misappropriating refunds, or abusing access to confidential information.

In two separate letters issued to SSA management, the IG and its contractor made recommendations to address the weaknesses reported in November 1997. SSA agreed with the majority of the recommendations in the first letter and has developed related corrective action plans. The Administration is still reviewing the second set of recommendations and planning related corrective actions.

Department of Veterans Affairs

The Department of Veterans Affairs (VA) relies on a vast array of computer systems and telecommunications networks to support its operations and store the sensitive information the department collects in carrying out its mission. In September 1998, we reported that general computer control weaknesses placed critical VA operations, such as financial management, healthcare delivery, benefit payments and life insurance services at risk of

[9]Social Security Accountability Report for Fiscal Year 1997, SSA Pub. No. 31-231, November 1997.

misuse and disruption.[10] In addition, sensitive information contained in VA's systems, including financial transaction data and personal information on veteran medical records and benefit payments, was vulnerable to inadvertent or deliberate misuse, fraudulent use, improper disclosure, or destruction—possibly occurring without detection.

VA operates the largest healthcare delivery system in the United States and guarantees loans on about 20 percent of the homes in the country. In fiscal year 1997, VA spent over $17 billion on medical care and processed over 40 million benefit payments totaling over $20 billion. The department also provided insurance protection through more than 2.5 million policies that represented about $24 billion in coverage at the end of fiscal year 1997. In addition, the VA systems support the department's centralized accounting and payroll functions. In fiscal year 1997, VA's payroll was almost $11 billion, and the centralized accounting system generated over $7 billion in additional payments.

In our report, we noted significant problems related to the department's control and oversight of access to its systems. VA did not adequately limit the access of authorized users or effectively manage user identifications and passwords. The department also had not established effective controls to prevent individuals, both internal and external, from gaining unauthorized access to VA systems. VA's access control weaknesses were further compounded by ineffective procedures for overseeing and monitoring systems for unusual or suspicious access activities.

In addition, the department was not providing adequate physical security for its computer facilities, by not assigning duties in such a way as to segregate incompatible functions, controlling changes to powerful operating system software, or updating and testing disaster recovery plans to prepare its computer operations to maintain or regain critical functions in emergencies. Many of these access and other general computer control weaknesses were similar to weaknesses that had been previously identified by VA's Office of Inspector General and consultant evaluations.

A primary reason for VA's continuing general computer control problems is that the department does not have a comprehensive computer security planning and management program. An effective program would include guidance and procedures for assessing risks and mitigating controls, and monitoring and evaluating the effectiveness of established controls.

[10]VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

In our report to VA, we recommended that the Secretary direct the CIO to (1) work with the other VA CIOs to address all identified computer control weaknesses, (2) develop and implement a comprehensive departmentwide computer security planning and management program, and (3) monitor and periodically report on the status of improvements to computer security throughout the department. In commenting on this report, VA agreed with these recommendations and stated that the department would immediately correct the identified computer control weaknesses and was developing plans to correct deficiencies previously identified by the VA IG and by internal evaluations.

Department of State

In May 1998, we reported that the Department of State did not have a program for comprehensively managing the information security risks associated with its many sensitive operations.[11] State relies on numerous decentralized information systems and networks to carry out its worldwide responsibilities and support business functions. Unclassified data stored in these systems are sensitive and make an attractive target for individuals and organizations desiring to learn about and damage State operations. For example, computerized information on Americans and Foreign Service Nationals, such as personnel records, pay data, private health records, and background investigation information about employees being considered for national security clearances could be useful to foreign governments wishing to build personnel profiles, and its disclosure might unnecessarily endanger State employees.

Despite its reliance on computers, State (1) lacked a central security management group to oversee and coordinate security activities, (2) did not routinely perform risk assessments so that its sensitive information could be protected based on its sensitivity, criticality, and value, (3) relied on a primary information security policy document that was outdated and incomplete, (4) did not adequately ensure that computer users were fully aware of risks and of their responsibilities for protecting sensitive information, and (5) lacked key controls for monitoring and evaluating the effectiveness of its security program, including procedures for responding to security incidents.

We also noted that State's information systems and the information contained within them were vulnerable to access, change, disclosure, disruption or even denial of service by unauthorized individuals. Our

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

penetration tests, which were designed to determine how susceptible State's systems were to unauthorized access, revealed that it was possible to access sensitive information. Further, these tests went largely undetected, further underscoring the department's serious vulnerability. As a result, individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses.

In our report to State, we made a variety of recommendations directed toward improving the department's management of its information security efforts and assisting State in developing a comprehensive information security program. State formally acknowledged weaknesses in its information security management and generally agreed with our recommendations. Senior State managers say that their commitment to improving information security has increased but that fully implementing our recommendations will require time and resources.

Department of Justice

In September 1997, the Department of Justice IG reported serious departmentwide computer-based control weaknesses that jeopardized a number of sensitive operations.[12] Access controls were weak over files supporting various operations at the Federal Bureau of Investigation, Drug Enforcement Administration, Immigration and Naturalization Service, and the U.S. Marshals Service. User passwords were not required to be changed, security software was not configured to prevent access by inactive users, system programmers had been inappropriately provided the ability to make numerous types of modifications to files that would allow them to circumvent security controls or assist others in such actions. Program change control procedures for system and application software were not formally documented or uniformly followed, increasing the risk that unauthorized software changes or unintentional errors could be made. Further, the IG reported that the department did not have a plan to recover primary systems, critical data processing applications, or key business processes in the event of a disaster. An underlying problem was that written security policies and procedures were outdated and did not define the roles and responsibilities of managers and others with security responsibilities. The Department of Justice management agreed with the findings and has stated that each departmental component will work with Justice's CIO to develop corrective actions.

[12]U.S. Department of Justice Annual Financial Statement for Fiscal Year 1996 (DOJ/OIG-97-24B, September 1997).

Other Federal Operations

Examples of risks at other agencies include the following:

- In May 1998, we reported that weak computer security practices at the Federal Aviation Administration (FAA) jeopardize flight safety.[13] FAA's air traffic control network is an enormous, complex collection of interrelated systems, including navigation, surveillance, weather, and automated information processing and display systems that reside at, or are associated with, hundreds of facilities. All the critical areas included in our review—facilities physical security, operational systems information security, future systems modernization security, and management structure and policy implementation were ineffective. For example, in the physical security area, a March 1997 inspection of one facility that controls aircraft disclosed 13 physical security weaknesses, including unauthorized personnel being granted unescorted access to restricted areas. FAA is unaware of the weaknesses and vulnerabilities that may currently exist at other locations because the agency has not assessed the physical security controls at 187 facilities since 1993. When we met with FAA officials in late July 1998, they acknowledged that major improvements are needed in all areas of FAA's security program and discussed preliminary efforts to address most of our recommendations.
- In April 1997, the Department of Transportation's IG identified multiple security exposures in the Department's extended wide area network which connects hundreds of local area networks and 50,000 computer workstations that support operations throughout the department, including the Federal Aviation Administration, Federal Highway Administration, United States Coast Guard, Federal Railroad Administration, National Highway Safety Traffic Administration as well as DOT headquarters.[14]
- In April 1997, the Department of Housing and Urban Development's IG identified a variety of weaknesses that affected systems critical to supporting all facets of the department's operations, including providing (1) housing subsidies for low and moderate income families, (2) grants to states and communities, and (3) direct loans for construction and rehabilitation of housing projects.[15] In particular, weaknesses associated with an application that annually processed over $9 billion in disbursements increased the risk of over or underpayments to housing

[13]Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155 May 18, 1998).

[14]Report on the Department of Transportation Fiscal Year 1996 Consolidated Financial Statement (AD-OT-7-004, April 10, 1997).

[15]Audit of the U.S. Department of Housing and Urban Development's Fiscal Year 1996 Financial Statements (97-FO-177-0003, April 10, 1997).

authorities, inaccurate budget projections, and users maliciously entering unauthorized transactions for payments.

- In July 1997, the audit of the Department of Education's fiscal year 1996 and 1995 financial statements reported access control weaknesses in the Payment Management System, which controlled disbursements of over $28 billion annually. As a result, unauthorized users could potentially have accessed confidential data, changed data, made unauthorized payments, or disabled the system.[16]
- In April 1997, the Department of the Interior's IG reported[17] that the Bureau of Indian Affairs' had not implemented an effective system security program for the Bureau's major and sensitive mainframe applications, including the Land Records Information System and the Individual Indian Monies System, that processed approximately 2.5 million transactions weekly. In particular, the Bureau had inadequate (1) access controls over the mainframe computers, (2) software development and change controls, and (3) segregation of duties for the systems support functions, including data administration, data security, and quality assurance/testing. In addition, a service continuity plan had not been developed and the off-site storage facility was not secure or environmentally protected.
- In March 1997, the Department of Commerce Inspector General reported material weaknesses at several Commerce Bureaus. For example, the Economic Development Administration, which managed a $1 billion grant program in fiscal year 1997, did not adequately segregate programming responsibilities or adequately restrict access to its informatio. systems. Inappropriately segregated duties can lead to implementation of unauthorized or inadequately tested programs. Further, unrestricted access can lead to accidental or intentional changes to program data.[18]

Recommended corrective actions have been provided to each of these agencies, and many have begun to implement them.

[16]U.S. Department of Education Fiscal Years 1996 and 1995 Financial Statements and Accompanying Notes, Price Waterhouse, LLP July 31, 1997.

[17]Audit Report on General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (Number 97-I-771, April 30, 1997).

[18]The U.S. Department of Commerce Consolidating Financial Statements Fiscal Year 1996 (Audit Report No FSD-9355-7-0001, March 1997) (attachment I, Department of Commerce IG report, Economic Development Administration report, p. 5).

Although Nature of Risks Vary, Control Weaknesses Across Agencies Are Similar

Although the nature of agency operations and the related risks vary, there are striking similarities in the specific types of general control weaknesses reported and in their serious negative impact on an agency's ability to ensure the integrity, availability, and appropriate confidentiality of its computerized operations. In many cases, agencies have developed policies and begun to implement control techniques that could provide effective security. However, they have not yet done enough to ensure that these policies and controls remain effective on an ongoing basis. The following sections describe each of the six areas of general controls and the specific weaknesses that were most widespread at the agencies covered by our analysis.

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 found that poor security planning and management was a widespread problem. Of 17 agencies where this aspect of security was reviewed, all had deficiencies. Many agencies had not developed security plans for major systems based on risk, had not formally documented security policies, and had not implemented a program for testing and evaluating the effectiveness of the controls they relied on. Examples include the following.

- In August 1997, the IG at the Department of Health and Human Services reported that the Health Care Financing Agency had not reviewed internal controls or developed security plans for its computer center, telecommunications networks, or significant applications. Further, it did not have a consistent set of policies for overseeing the effectiveness of security at its contractor locations.[19]
- In July 1997, the Department of the Treasury IG reported that the Bureau of Alcohol, Tobacco and Firearms had not developed formal policies, standards, and procedures; had not established a formal program for

[19]Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-00001, August 29, 1997).

security awareness and training; and had not identified all of its major applications.[20]

- In April 1997, we reported that the Internal Revenue Service needed to strengthen computer security management and that its approach to computer security was not effective in preventing serious and persistent computer security control weaknesses that exposed tax processing operations to the serious risk of disruption and taxpayer data to the risk of unauthorized use, modification, and destruction.[21]
- In May 1997, independent auditors recommended that the Office of Personnel Management develop security plans, identify system owners, and require periodic independent reviews of security controls.[22]
- In May 1996, we reported that the Department of Defense needed to establish a more comprehensive information systems security program. Specific weaknesses included (1) outdated and incomplete policies for detecting and reacting to computer attacks, (2) lack of awareness among computer users, and (3) inadequately trained system and network administrators.[23]

As a result of these types of deficiencies, agencies (1) were not fully aware of the information security risks to their operations, (2) had accepted an unknown level of risk by default rather than consciously deciding what level of risk was tolerable, (3) had a false sense of security because they were relying on controls that were not effective, and (4) could not make informed judgments as to whether they were spending too little or too much of their resources on security. Security program management is discussed in greater detail in chapter 3.

Access Controls

Access controls limit or detect inappropriate access to computer resources (data, equipment, and facilities) thereby protecting these resources against unauthorized modification, loss, and disclosure. Access controls include physical protections, such as gates and guards, as well as logical controls, which are controls built into software that (1) require users to authenticate themselves through the use of secret passwords or

[20] Audit of the Bureau of Alcohol, Tobacco, and Firearms Fiscal Years 1996 and 1995 Financial Statements (OIG-97-084, July 9, 1997).

[21] IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997).

[22] Financial Statements, Fiscal Year 1996, U.S. Office of Personnel Management, Independent Auditors' Report (May 30, 1997).

[23] Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

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. Without adequate access controls, unauthorized individuals, including outside intruders or terminated employees, can surreptitiously read and copy sensitive data and make undetected changes or deletions for malicious purposes or personal gain. In addition, authorized users could unintentionally modify or delete data or execute changes that are outside of their span of authority.

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

Access control weaknesses were reported for all 23 of the agencies for which this area of controls was evaluated. Specific common problems included the following.

- Managers had not precisely identified access needs for individual users or groups of users. Instead, they had provided overly broad access privileges to very large groups of users. As a result, far more individuals than necessary had the ability to browse and, sometimes, modify or delete sensitive or critical information. At one agency, for instance, a number of interconnected systems with very poorly implemented access controls were accessible from remote locations by anyone who had the telephone number for the supporting network. Because access controls associated with both the network and the systems were weak, an anonymous intruder could easily have dialed into the network, accessed any one of several systems, and committed any number of malicious actions, including reading, modifying, and deleting both data and other users' access rights and severely disrupting service. At another agency, 90 employees could change amounts available to grantees and contractors associated with an $8 billion grant program.

- Access was not appropriately authorized and documented. For example, at one agency, user access was verbally requested and approved and no related documentation was maintained.
- Users shared accounts and passwords or posted their passwords in plain view, making it impossible to trace specific transactions or modifications to an individual. Also, use of default, easily guessed, and unencrypted passwords significantly increased the risk of unauthorized access.
- Software access controls were improperly implemented, resulting in unintended access or gaps in access control coverage. For example, at one agency location, any one of 17,000 system users could search, view, and print information in any of the other users' print files because access to temporary files holding users' output was not adequately restricted.
- User activity was not adequately monitored to deter and identify inappropriate actions, and when suspicious activity was noticed, it was often not investigated nor the perpetrator penalized. For example, records of user activity, referred to as audit logs, were either not maintained, not maintained in a useable format, or were too voluminous to be practical. As a result, it was either not possible or practical to review these logs to identify inappropriate actions and link any such actions to individual users. Such monitoring is especially important to prevent users with access to sensitive data from inappropriately browsing data that do not pertain to the work at hand and to identify activity indicating an intrusion into a network or system. However, tests showed that most attacks at this agency were not detected and reported.
- Access was not promptly terminated when users either left the agency or adjusted when their responsibilities no longer required them to have access to certain files. In addition, inactive user identifications were not routinely identified and deleted. As a result, contractors and former employees who were no longer associated with the agency, could still read, modify, copy, or delete data, and employees who changed positions within an agency had access to files that were not needed in their new positions. For example, at one location, automated controls were set to allow former employees access for 90 days after their employment had terminated.

To illustrate the risks associated with poor authentication and access controls, in recent years, we have begun to incorporate penetration testing into our audits of information security. Such tests involve attempting to gain unauthorized access to sensitive files and data by searching for ways to circumvent existing controls, often from remote locations. Unfortunately, our auditors have been successful, in almost every test, in

readily gaining unauthorized access that would allow intruders to read, modify, or delete data for whatever purpose they had in mind.

Application Software Development and Change Controls

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

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

The effectiveness of software change controls is of particular concern as agencies design, test, and implement changes to ensure that their computer software will properly handle the year-2000 date change. As the end of the millennium approaches, agencies are under increasing pressure to ensure that their computers can distinguish between the year 1900 and the year 2000, since many use only the last two digits when identifying years. In an effort to accomplish these changes on time, agencies may be forced to speed up their software change process and increase their reliance on newly hired personnel or contractors. In such an environment, it will be especially important to ensure that software changes are properly tested and approved before they are implemented.

Weaknesses in software program change controls were identified for 14 of the 18 agencies where such controls were evaluated. The most common types of weaknesses in this area included the following:

- Testing procedures were undisciplined and did not ensure that implemented software operated as intended. For example, at one agency, changes were made directly to software programs in operation rather than in a separate and controlled test environment, increasing the risk that

erroneous or unauthorized software would result in miscalculations of pension liability.

- Implementation procedures did not ensure that only authorized software was used. In particular, procedures did not ensure that emergency changes were subsequently tested and formally approved for continued use and that implementation of "locally-developed" unauthorized software programs was prevented or detected.
- Access to software program libraries was inadequately controlled. For example, at one agency, most system users—over 13,000 individuals—had the ability to modify application programs that processed millions of dollars in financial transactions. At another agency, approximately 16,000 users had unrestricted access to application programs, which allowed them to modify and delete programs and data.

Segregation of Duties

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

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

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

Controls to ensure appropriate segregation of duties consist mainly of documenting, communicating, and enforcing policies on group and individual responsibilities. Enforcement can be accomplished by a

combination of physical and logical access controls and by effective supervisory review.

Segregation of duties was evaluated at 17 of the 24 agencies covered by our analysis. Weaknesses were identified at 16 of these agencies. Common problems involved computer programmers and operators who were authorized to perform a wide variety of duties, thus providing them the ability to independently modify, circumvent, and disable system security features. For example, at one data center, a single individual could independently develop, test, review, and approve software changes for implementation. Segregation of duty problems also were identified related to transaction processing. For example, at one agency, all users of the financial management system could independently perform all of the steps needed to initiate and complete a payment—obligate funds, record vouchers for payment, and record checks for payment—making it relatively easy to make a fraudulent payment.

System Software Controls

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

Controls over access to and modification of system software are essential in providing reasonable assurance that operating system-based security controls are not compromised and that the system will not be impaired. If controls in this area are inadequate, unauthorized individuals might use system software to circumvent security controls to read, modify, or delete critical or sensitive information and programs. Also, authorized users of the system may gain unauthorized privileges to conduct unauthorized actions or to circumvent edits and other controls built into application programs. Such weaknesses seriously diminish the reliability of information produced by all of the applications supported by the computer system and increase the risk of fraud, sabotage, and inappropriate

disclosures. Further, system software programmers are often more technically proficient than other data processing personnel and, thus, have a greater ability to perform unauthorized actions if controls in this area are weak.

The control concerns for system software are similar to the access control issues and software program change control issues discussed earlier in this section. However, because of the high level of risk associated with system software activities, most entities have a separate set of control procedures that apply to them.

Operating system software controls were covered in audits for only 9 of the 24 agencies included in our review. However, problems were identified for all 9 agencies, illustrating the importance of reviewing operating system controls. A common type of problem reported was insufficiently restricted access that made it possible for knowledgeable individuals to disable or circumvent controls in a wide variety of ways. For example, at one facility, 88 individuals had the ability to implement programs not controlled by the security software and 103 had the ability to access an unencrypted security file containing passwords for authorized users.

Service Continuity Controls

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

Although often referred to as disaster recovery plans, controls to ensure service continuity should address the entire range of potential disruptions. These may include relatively minor interruptions, such as temporary power failures or accidental loss or erasing of files, as well as major disasters, such as fires or natural disasters that would require reestablishing operations at a remote location.

Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an agency's ability to

accomplish its mission. If controls are inadequate, even relatively minor interruptions can result in lost or incorrectly processed data, which can cause financial losses, expensive recovery efforts, and inaccurate or incomplete financial or management information. Service continuity controls include (1) taking steps, such as routinely making backup copies of files, to prevent and minimize potential damage and interruption, (2) developing and documenting a comprehensive contingency plan, and (3) periodically testing the contingency plan and adjusting it as appropriate.

Service continuity controls were evaluated for 20 of the agencies included in our analysis. Weaknesses were reported for all of these agencies. Common weaknesses included the following:

- Plans were incomplete because operations and supporting resources had not been fully analyzed to determine which were the most critical and would need to be resumed as soon as possible should a disruption occur. For example, one agency had identified critical workloads and processing priorities that would need to be resumed and supported after a disruption but had not identified the specific software needed for users to perform their jobs. Such information could be difficult to compile in the confusion that would be likely after a major disruptive event.
- Disaster recovery plans were not fully tested to identify their weaknesses. One agency's plan was based on an assumption that key personnel could be contacted within 10 minutes of the emergency, an assumption that had not been tested.

Conclusion

Important operations at every major federal agency are at some type of risk due to weak information security controls. There are many specific causes of these weaknesses, but many result from poor security program management and poor administration of available control techniques.

The audit reports cited in this chapter include numerous recommendations to individual agencies that address the specific weaknesses reported. For this reason, we are making no additional recommendations to these agencies in this report. However, our executive guide, Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68), discusses the results of our recent study of information security best practices and outlines a number of principles and practices that could enable federal agencies to implement more

effective information security programs. Chapter 3 summarizes the principles outlined in the executive guide.

Need for Improved Security Program Planning and Management at Individual Agencies

Although auditors can provide periodic independent assessments of agency operations, ultimately it is agency management that is responsible for ensuring that internal controls, including information security controls, are appropriately selected and effectively implemented on an ongoing basis. In September 1996, we reported that an underlying cause of poor federal information security was that many agencies had not instituted a framework for proactively managing the information security risks associated with their operations.[1] Instead, there was a tendency to react to individual audit findings as they were reported, with little ongoing attention to the systemic causes of control weaknesses. Since then, as discussed in chapter 2, additional audits have identified the same underlying problem. Security program planning and management deficiencies were reported for 17 of the 24 agencies included in our analysis. In particular, agencies were not adequately assessing risks and monitoring control effectiveness.

To identify potential solutions to this problem, during 1997, we studied the security management practices of eight nonfederal organizations known for their superior security programs. We found that these organizations managed their information security risks through a cycle of risk management activities, and we identified 16 specific practices that supported these risk management principles. These findings were initially published as an exposure draft in November 1997. Subsequently, they were published in May 1998 in an executive guide entitled Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68). The guide is generally consistent with OMB and NIST guidance on information security program management, and it has been endorsed by the CIO Council as a useful resource for agency managers. The guide's major points are summarized below.

Best Practices Provide a Framework for Improvement

Our study of information security management practices identified a fundamental set of management principles and 16 specific practices. Together, these principles and practices constitute a cycle of activity for managing risk.

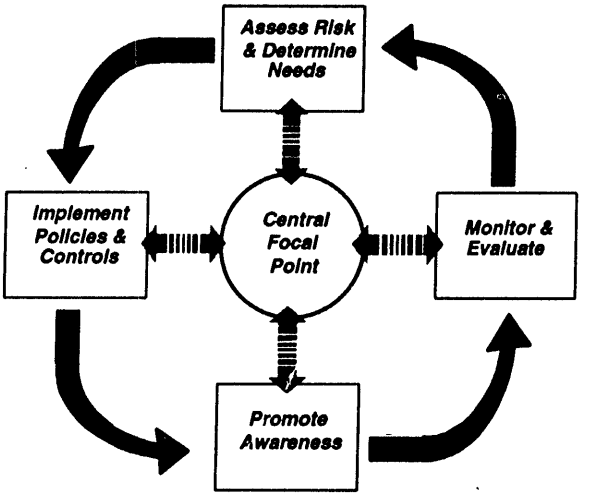
The Risk Management Cycle

The risk management cycle, as depicted in figure 3.1, begins with an assessment of risk and determination of needs, including selecting cost-effective policies and related controls. Once policies and controls are decided on, they must be implemented. Then, policies and controls, as

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

well as the risks that prompted their adoption, must be communicated to those responsible for complying with them. Finally, and perhaps most importantly, there must be procedures for evaluating the effectiveness of policies and related controls and reporting the resulting conclusions to those who can take appropriate corrective action. Also, our study found that a strong central security management 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. This cycle of activity, coordinated by a central focal point, can help ensure that existing controls are effective and that new, more advanced control techniques are prudently and effectively selected and implemented.

Figure 3.1: The Risk Management Cycle



The elements of the risk management cycle are not new. They have been described in various ways in OMB and NIST guidance and in various other guides on information security and internal controls. Nevertheless, as

basic as these principles are, audits continue to show that many federal agencies have not implemented this cycle of activity.

One possible cause for this deficiency is that some senior agency officials, like many private sector executives, may be just beginning to realize how critical their information resources are to their program operations and may not fully understand that security weaknesses present formidable risks to mission-related operations. Another reason is that maintaining adequate information security can be difficult. The complicated and technical nature of many of the risks and controls requires that organizations adopt more defined processes than are needed to manage other types of internal controls. These defined processes are needed to ensure that personnel with the right mix of expertise are involved in risk management decisions; that all pertinent factors are considered; that the effectiveness of controls, especially technical controls, is reliably evaluated; and that the results of these evaluations and their potential effects on critical operations are clearly reported to senior officials.

Within this basic risk management cycle, we identified 16 practices that were key to the effectiveness of an information security program. A brief description of these practices, organized according to the five elements of the risk management cycle, follows. A more detailed description accompanied by case examples can be found in our executive guide.

Assess Risk and Determine Needs

Practice 1: Recognize Information Resources as Essential Organizational Assets

Organizations that have become heavily dependent on computers, electronic data, and telecommunications to conduct their activities must recognize that these information resources are critical assets, essential to supporting business operations. Information protection should be viewed as an integral element of operational management and strategic planning. In particular, senior executives must understand the importance of data and systems and be willing to devote an appropriate level of resources to protecting these assets.

Practice 2: Develop Practical Risk Assessments That Link Security to Business Needs

Security needs should be based on risk, and this requires some type of risk assessment. Various methods can be used, from relatively informal discussions to complex analyses. Key success factors are that risk assessments

- be required and involve defined minimum procedures;
- involve a mix of individuals with knowledge of business operations and technical aspects of the organization's systems;
- rank, but not necessarily precisely quantify, risks;
- require sign-off by business managers indicating agreement with risk reduction decisions and acceptance of the residual risk; and
- result in documentation that is provided to more senior officials and internal auditors, so that participants can be held accountable for their decisions.

Practice 3: Hold Program and Business Managers Accountable	Primary responsibility for managing risk should rest with business or program managers because they are in the best position to determine what the business impact of a loss of integrity, confidentiality, or availability of information resources would be. The security specialists, on the other hand, should play more of an educational and advisory role. However, they should not hesitate to elevate discussions to higher levels if they believe that inappropriate risk management decisions are being made.
Practice 4: Manage Risk on a Continuing Basis	Risk must be continuously reassessed because the factors that affect risk —threats, technology, known vulnerabilities, and the sensitivity of the operations being supported—frequently change.

Establish a Central Management Focal Point

Practice 5: Designate a Central Group to Carry Out Key Activities	Central security management groups can ensure that the various elements of the risk management cycle are implemented. They can also serve as a conduit for communicating information across organizational lines and from outside sources.
Practice 6: Provide the Central Group Ready and Independent Access to Senior Executives	Regardless of their organizational position, an organization's central security manager must feel that he or she can comfortably raise issues to higher levels. Independent access to senior executives allows senior security managers to provide an objective assessment of security needs and gives them the clout to be effective throughout their organizations.
Practice 7: Designate Dedicated Funding and Staff	Central groups should have defined budgets that allow them to plan and set goals. However, they may also rely on a network of subordinate security specialists who work in other organizational units.

Practice 8: Enhance Staff Professionalism and Technical Skills	Develop security managers into a cadre of respected specialists. Technical training and professional certification should be encouraged and kept current.

Implement Appropriate Policies and Related Controls

Practice 9: Link Policies to Business Risks	Policies and the controls to implement policies should flow directly from risk assessments and, thus, be linked to business risks. Also, as risk factors change, policies and controls should be updated.
Practice 10: Distinguish Between Policies and Guidelines	Distinguishing between policies and guidelines provides flexibility for individual business units. However, high-risk operations are likely to require a more detailed set of mandatory policies and standards.
Practice 11: Support Policies Through the Central Security Group	Central groups can promote consistency in policy implementation by developing the related written documents, based on input from business managers, attorneys, and others, and by serving as the organizational focal point for policy questions.

Promote Awareness

Practice 12: Continually Educate Users and Others on Risks and Related Policies	Awareness of both risks and policies should be vigorously promoted so that users understand the importance of complying with policies and controls. In particular, sensitizing employees and other users to risks can make users (1) think twice before revealing sensitive data and (2) more likely to notice and report suspicious activity.
Practice 13: Use Attention-Getting and User-Friendly Techniques	Various promotion techniques, such as intranet websites, awareness days, and posters can keep security in the forefront of users' minds. Two effective techniques are customized briefings to individual business units and videos featuring top organization executives promoting security as everyone's responsibility.

Monitor and Evaluate Policy and Control Effectiveness

Practice 14: Monitor Factors That Affect Risk and Indicate Security Effectiveness

Managers should develop procedures for periodically evaluating the effectiveness of their information security programs, paying closest attention to the controls associated with the most critical operations. Monitoring and evaluation efforts should focus primarily on (1) determining if controls are operating as intended and (2) evaluating the effectiveness of the security program in communicating policies, raising awareness levels, and reducing incidents. Testing controls, including penetration testing, is an effective way to determine if policies and controls are operating effectively. Other types of monitoring and evaluation activities include periodic reports on compliance with various policies, the number of inquiries from users, and the number and nature of security incidents reported.

Practice 15: Use Results to Direct Future Efforts and Hold Managers Accountable

The full benefits of monitoring are not achieved unless results are reported to officials who can take any actions needed to improve the security program. Such action can include (1) reassessing previously identified risks, (2) identifying new problem areas, (3) reassessing the appropriateness of existing controls and security-related activities, (4) identifying the need for new controls, (5) redirecting subsequent monitoring efforts, and (6) holding managers accountable for compliance. Effecting change and holding managers accountable generally requires involvement of an organization's most senior executives.

Practice 16: Be Alert to New Monitoring Tools and Techniques

Because new technology is being introduced at a fast pace, with related security controls often lagging behind, security specialists must keep abreast of information on new risks and control techniques through professional organizations and literature.

Improved Security Depends on Broader Improvements to Information Technology Management

The risk management activities described in our executive guide and summarized above are likely to be most successful if implemented in the context of broader improvements to federal information technology management. Over the last few years, the Congress has enacted legislation that is prompting landmark reforms in this broader area. In particular, the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 emphasize the need for agencies to apply information resources to effectively support agency missions and delivery of services to the public.

These laws stress the importance of involving senior executives in information management decisions, appointing senior-level chief information officers, and using performance measures to assess the contribution of technology in achieving mission results. Both specify security as an aspect of information management that must be addressed. These broader information management improvements are apt to improve security management because they prompt senior agency officials to take a more active role in managing their organizations' use of information technology. Further, agencies may find this environment of reform conducive to rethinking their security programs and considering new practices.

Conclusion

Although existing federal guidance outlines basic security planning and management requirements, many, if not most, of the reported weaknesses in agency information security controls can be traced to poor performance in this area. Good management is essential to ensure that relied-upon controls are working effectively on a continuous basis. It is also important to help ensure that agencies promptly identify emerging risks and take full advantage of more sophisticated security controls as they become available. Our executive guide, which outlines the risk management practices employed by leading organizations, provides a framework of solutions that supplement existing federal guidance and can assist agencies in strengthening their management of this critical area.

Chapter 4

Centrally Directed Improvement Efforts Have Increased, but Most Have Not Progressed Beyond Planning Stage

Several new governmentwide efforts to improve federal information security have been initiated since we last reported on this topic in September 1996, such as the recent issuance of Presidential Decision Directive (PDD) 63 on critical infrastructure protection. Most of these efforts, however, had only recently been started and had not progressed far beyond the planning stages at the close of our review. In addition, while these efforts address some important information security problems, such as inadequate risk awareness and incident reporting capabilities, none provides a comprehensive strategy for adequate monitoring and oversight of agency performance in this area.

Federal agencies are primarily responsible for protecting their respective information resources, but governmentwide leadership, coordination, and oversight are important to (1) ensure that federal executives understand the risks to their operations, (2) monitor agency performance in mitigating these risks, (3) ensure implementation of needed improvements, and (4) facilitate actions to resolve issues affecting multiple agencies. To help achieve this, the Paperwork Reduction Act of 1980 made OMB responsible for developing information security policies and overseeing related agency practices.

Since September 1996, OMB has continued to review selected agency system-related projects and provide input through various federal task forces and working groups. These efforts were supplemented in late 1997 when the CIO Council, under OMB's leadership, designated information security as one of six priority areas and established a Security Committee. The Committee, in turn, has developed a preliminary plan and taken several actions primarily related to promoting awareness, planning for improving agency access to incident response services, and establishing links with other federal entities involved in security issues. However, neither OMB nor the Council has developed a comprehensive strategy for ensuring that agency security programs are effective.

More recently, in May 1998, PDD 63 was issued, which established several entities within the National Security Council, the Department of Commerce, and the Federal Bureau of Investigation to address critical infrastructure protection, including federal agency information infrastructures. This directive specified several requirements related to evaluating and coordinating federal agency information security practices. However, at the close of our review in early August 1998, it was not clear how and when these new requirements would be implemented and how

they would be coordinated with existing requirements and with efforts underway at other federal entities.

Previous Recommendations Urged More Active Oversight

In 1996, we reported that, although OMB had improved federal guidance pertaining to information security, its oversight efforts were uneven, and it generally did not proactively attempt to identify and promote resolution of fundamental security program weaknesses that were likely to be at the root of reported deficiencies at individual agencies. Our report recommended that OMB

- take advantage of the wide range of information currently reported in financial statement audit reports and agency self-assessments to monitor agency compliance with OMB's guidance and the effectiveness of agency information security programs, and
- implement a program for increasing its program examiners' understanding of information security management issues so that they can more readily identify and understand the implications of information security weaknesses on agency programs.

We also recommended that OMB promote the CIO Council's (1) adoption of information security as one of its top priorities and (2) development of a strategic plan for increasing awareness of the importance of information security, especially among senior agency executives, and improving information security program management governmentwide. We suggested that the CIO Council's strategic plan include plans for

- developing information on the existing security risks associated with nonclassified systems currently in use,
- developing information on the risks associated with evolving practices, such as Internet use,
- identifying best practices regarding information security programs so that they can be adopted by federal agencies,
- establishing a program for reviewing the adequacy of individual agency information security programs,
- ensuring adequate review coverage of agency information security practices by considering the scope of various types of audits and reviews performed and acting to address any identified gaps in coverage,
- developing or identifying training and certification programs that can be shared among agencies, and
- identifying proven security tools and techniques.

CIO Council Plans Focus on Solving Selected Crosscutting Problems

The CIO Council has begun to lay the groundwork for improvements in several areas, but has not developed a comprehensive strategy that identifies the most critical issues affecting federal information security and includes long-term goals and objectives, including annual performance goals. During 1997, the Council discussed various critical information management issues, and in late 1997, formally declared information security as one of six priority areas that will guide the Council's activities. The stated goal for this area is to "ensure implementation of security practices within the Federal Government that gain public confidence and protect Government service, privacy, and sensitive and national security information." Two other priority areas—defining an interoperable architecture and improving information technology workforce skills—may also support security improvements. An interoperable federal computer systems architecture will make it easier to implement and manage security controls, and improving technical workforce skills will help provide expertise needed to select and properly implement technical controls.

To guide activities associated with its information security goal, the Council established the Security Committee, also in late 1997. Since then, the Committee has taken some steps to coordinate its plans with related activities at other federal entities and address some of the most prominent governmentwide problems associated with information security, such as insufficient awareness of risks, inadequate technical training, and poor incident response capabilities. These projects have been conducted during monthly meetings and by part-time efforts of individual committee members between meetings. Accomplishments as of August 1998 are described below.

Preliminary Strategic Plan Developed

During late 1997, the Security Committee developed a preliminary strategic plan, which was incorporated into a larger strategic information technology management plan developed jointly by OMB and the CIO Council and issued in January 1998.[1] The information security segment of the plan includes three general objectives: promote awareness and training, identify best practices, and address technology and resource issues. Under each of these objectives, three or four specific activities and related milestones are briefly identified. Committee members told us that they expect to expand on this initial plan as the year progresses.

[1]The Paperwork Reduction Act requires OMB to annually submit a governmentwide information technology plan to the Congress. The 1998 plan is the first such plan jointly prepared by OMB and the CIO Council.

Expansion of the plan is important to help ensure that the many facets of this problem are identified, prioritized, and addressed efficiently and effectively. Ideally, such a plan would identify the many policy, technical, legal, and human resource issues that affect federal information security and describe the various roles and activities of other federal entities involved in improving the protection of unclassified federal data. Such entities include, but are not limited to, NIST, the National Security Agency, and the Government Information Technology Services Board. A description of the information security-related activities of OMB's Office of Information and Regulatory Affairs, Office of Federal Financial Management, and program examiners also would be useful. Further, the plan could include long-term goals and objectives, including time frames, priorities, and expected accomplishments, and annual performance goals.

For example, to better coordinate agency activities, increase efficiency, and build on existing expertise, the plan could provide for identifying and sharing individual agency solutions to common challenges, such as incident handling, investigations, contingency planning, security plan development, virus protection, security awareness, and system architecture design. Related efforts could include, for each functional area,

- designating an individual to serve as a focal point;
- developing a consolidated e-mail directory for key agency personnel;
- identifying useful web sites and evaluation tools;
- publicizing software and training aids and opportunities; and
- reviewing, filtering, and distributing notices and advisories on software vulnerabilities, such as those issued by Carnegie-Mellon University's Computer Emergency Response Team.

In addition to coordinating and optimizing the value of agency efforts, such a plan could help inform agency managers about their information security responsibilities, maximize the value of audit results, and facilitate administration and Congressional oversight. Further, it could provide support for the governmentwide performance plan that OMB is required to include in the president's annual budget submission to the Congress under the Government Performance and Results Act. The first governmentwide performance plan and related "priority management objectives" were published in early 1998 as part of the President's Fiscal Year 1999 Budget. However, that plan provided few details on the administration's strategy for addressing widespread deficiencies in federal information security.

Efforts to Facilitate Projects Sponsored by Others

The Security Committee has established links with other federal entities with information security responsibilities, including NIST and the National Security Agency; requested briefings on other federally sponsored information security efforts; and acted to support and facilitate these efforts. For example, in late 1997 and early 1998, the Committee explored ways to gain broader federal agency participation in FedCIRC, a program initiated by NIST in 1996 to provide agencies a means of responding to computer security incidents. OMB Circular A-130, Appendix III, requires agencies to have a capability to (1) help users when a security incident, such as a suspected system intrusion, occurs, (2) share information on common vulnerabilities and threats, and (3) assist in pursuing appropriate legal action. In May 1998, the Council took action on the FedCIRC issue by endorsing the Security Committee's recommendation to shift sponsorship of FedCIRC to GSA and to change the funding mechanism. As of August 1998, the Council was developing detailed arrangements in anticipation of implementing the change at the start of fiscal year 1999.

Other briefing topics at Security Committee meetings have included our study of information security management best practices, which is discussed in chapter 3, and the "Information Security Countermeasures Assessment Project," sponsored by the Air Force Research Laboratory. The latter is an effort to develop a better understanding of the effectiveness of administrative and technical measures for preventing security incidents.

Security Awareness Seminar

In February 1998, the Security Committee arranged for and held a security awareness seminar to brief federal officials on information security risks. Speakers included representatives from the National Security Agency, NIST, and private sector organizations who described the latest challenges to maintaining adequate security. The seminar was attended by about 80 individuals—primarily agency CIO and federal agency information security officers. Comments from seminar attendees indicated that the program was a success and that more such programs addressing an expanded variety of topics would be welcome.

The results of our recent study of information security management practices indicate that it would be valuable to expand the reach of such awareness seminars beyond agency CIO offices to a broader audience of senior program executives. If program officials have a more thorough understanding of the information security risks to their operations and assets, they will be more likely to (1) encourage their staff to comply with

security requirements, (2) devote resources for security, and (3) make prudent decisions regarding the appropriate levels of protection needed.

Oversight of Agencies Remains Limited

A major aspect of our previous recommendations that is not being addressed by either OMB or the CIO Council is establishing a more structured program for ensuring that agency security programs are adequately evaluated and the results used to measure performance and prompt improvement. Minimum requirements for agency security programs are outlined in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources." Updated in February 1996, Appendix III requires agencies to assign responsibility for security, develop a system security plan, screen and train individual users, assess risk, plan for disasters and contingencies, and periodically review their security safeguards. It also requires agencies to clearly define responsibilities and expected behavior for all individuals with access to automated systems and to implement security incident response and reporting capabilities.

Central oversight of the effectiveness of agency security programs is important because audit results indicate that agencies are not adequately identifying and addressing security weaknesses on their own. One resource for such oversight is the large body of audit evidence that has become available in the last few years, primarily due to reviews of computer security controls performed as part of financial statement audits. Although, as discussed in chapter 2, comprehensive audits of computer security are not yet being performed at all agencies, analyses of these audit results and related reports could provide a starting point for measuring progress. The results can also be useful in identifying continuing problem areas and encouraging agency managers to take a more proactive role in identifying and addressing weaknesses themselves—before the weaknesses are discovered and reported by auditors.

OMB's Oversight Efforts Focus on Individual Issues and Projects

OMB's program examiners may consider information security during their broader review of an agency's mission-related programs, generally, as part of their review of agency information technology investment plans. Program examiners are assisted in this area by policy analysts in OMB's Information Policy and Technology Branch. In addition to their own specialized expertise, these policy analysts keep abreast of governmentwide information security issues by interacting with other

federal entities such as the Federal Computer Security Managers Forum, the National Security Telecommunications and Information Systems Security Committee, the Security Policy Board, and the National Security Telecommunications Advisory Committee.

In 1996, we reported that few of the program examiners had significant experience or expertise in dealing with information systems or related security issues and most did not consider the effectiveness of an agency's overall information security program. For this reason, in our September 1996 report, we recommended that OMB implement a program for increasing its program examiners' understanding of information security management issues and of the related audit results that were available to them.

Since then, officials in OMB's Information Policy and Technology Branch say that they have provided two specialized security training sessions to program examiners and have continued to advise them on various security-related issues, such as the adequacy of system security plans, authentication, encryption, privacy of data and databases, and Internet and World Wide Web use. Agency projects cited as receiving attention pertaining to information security since early 1997 include (1) DOD's Defense Messaging System, (2) the FBI's National Crime Information Center information sharing initiative, (3) encryption of online services at the Departments of Education and the Interior and the Office of Personnel Management, and (4) critical infrastructure protection issues at the Federal Aviation Administration and the Departments of Energy and Defense.

A More Comprehensive and Structured Assessment Program Would Provide Benefits

While OMB's policy analysts and program examiners can provide valuable oversight of specific issues and projects, in light of the continuing reports of serious deficiencies, a more structured approach for measuring broader compliance with Circular A-130, Appendix III, and the effectiveness of agency security programs is needed. To be effective, such an approach must include comprehensive evaluations and tests of agency security programs at major agencies and reports at regular intervals that show improvements and deteriorations in program effectiveness.

Much could be learned by analyzing the results that are already available from financial statement audits, as discussed in chapter 2. Also, agency-initiated assessments, required by both OMB Circular A-130, Appendix III, and FMFIA, can be a source of evaluation results. Periodic

evaluations initiated by agency management are an essential step in helping determine whether controls are effective, which is an essential aspect of managing risk, as discussed in chapter 3. However, recent audits have identified numerous serious information security weaknesses that have apparently not been identified by agency managers and have not been reported in annual reports to the President and the Congress, as required by FMFIA. As a result, these reports are of limited value for oversight and, more importantly, agencies do not have the information they need to manage their information security risks.

To assist agencies in reviewing their computer-based controls and supplement audit information that is already available, OMB or the CIO Council could establish an independent cadre of experts to review critical areas of agency operations that are not being adequately evaluated. Such a cadre of experts could be created by drawing on the resources of many federal agencies, as we suggested in our September 1996 report, or a specialized unit could be established at an agency that already has a relatively high degree of expertise, such as NIST or the National Security Agency.

Regardless of how and by whom evaluations are conducted, results could be used to measure agency performance, identify recurring or longstanding problems, and identify gaps in audit coverage. For example, annual summary reports could be developed to show (1) the most commonly reported types of problems and (2) agencies where the same information security weaknesses were identified for more than 1 year. More refined performance indicators could distinguish between weaknesses classified as "material weaknesses" and those considered "reportable conditions," which are less serious than material weaknesses. These are standard classifications used in financial statement audit reports. OMB and the CIO Council could work with agency IGs, through the President's Council on Integrity and Efficiency, to develop other performance indicators. Such an annual "report card" could highlight improvements in agency performance as well as provide agencies an additional incentive to avoid being designated as an organization with long-standing information security problems.

PDD 63 Supplements Existing Requirements From a National Security Perspective

PDD 63 provides for additional central oversight of agency practices by the National Security Council in the Executive Office of the President. However, at the close of our review in August 1998, it was too early to determine how these provisions would be implemented, how effective they would be, and how they would be coordinated with ongoing efforts by the CIO Council and others.

In its October 1997 report, Critical Foundations: Protecting America's Infrastructures, the President's Commission on Critical Infrastructure Protection recognized the need for improved oversight of agency security practices and recommended assigning responsibility for oversight of federal systems security to a proposed Office of National Infrastructure Assurance within the National Security Council. As envisioned by the Commission, this Office would be given "overall program responsibility for infrastructure assurance matters, including policy implementation, strategy development, federal interagency coordination, and liaison with state and local governments and the private sector."

On May 22, 1998, PDD 63 established such an entity under the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, who is to report to the President through the Assistant to the President for National Security Affairs. This new entity, termed the Critical Infrastructure Coordination Group, is to be supported by a newly created Critical Infrastructure Assurance Office within the Department of Commerce.

The PDD addresses a range of national infrastructure protection issues and includes several provisions intended to ensure that critical federal computer, or "cyber-based," systems are protected from attacks by our nation's enemies. Specifically, it states that "the Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved" and that federal department and agency CIOs shall be responsible for information assurance. Although details are not provided, the Directive requires each department and agency to develop a plan within 180 days from the issuance of the Directive in May 1998 for protecting its own critical infrastructure, including its cyber-based systems. The Critical Infrastructure Coordination Group is then to sponsor an "expert review process" for those plans. Other key provisions related to the security of federal information systems include

- a review of existing federal, state, and local bodies charged with information assurance tasks;

- enhanced collection and analysis of information on the foreign information warfare threat to our critical infrastructures;
- establishment of a National Infrastructure Protection Center within the Federal Bureau of Investigation to facilitate and coordinate the federal government's investigation and response to attacks on its critical infrastructures;
- assessments of U. S. Government systems' susceptibility to interception and exploitation; and
- incorporation of agency infrastructure assurance functions in agency strategic planning and performance measurement frameworks.

Several of these provisions appear to overlap with existing requirements prescribed in the Paperwork Reduction Act of 1980, OMB Circular A-130, Appendix III, the Computer Security Act, the Clinger-Cohen Act, and the Federal Managers' Financial Integrity Act. In addition, some of PDD 63's objectives are similar to objectives being addressed by other federal entities, such as development of the FedCIRC program by NIST and the CIO Council. The relationship among these requirements and existing efforts had not been clarified at the conclusion of our review.

Conclusion

Since September 1996, the need for improved federal information security has received increased visibility and attention. However, central oversight has remained limited and a comprehensive strategy has not been developed. As a result, many aspects of the recommendations we made in September 1996 are still applicable. The CIO Council's efforts during late 1997 and the first half of 1998, as well as issuance of PDD 63 in May 1998, indicate that senior federal officials are increasingly concerned about information security risks, both to federal operations as well as to privately-controlled national infrastructures, and are now moving to address these concerns. Coordinated efforts throughout the federal community, as envisioned by PDD 63, will be needed to successfully accomplish the objectives of these efforts and substantively improve federal information security. It is especially important that a governmentwide strategy be developed that clearly defines and coordinates the roles of new and existing federal entities in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation and support.

Recommendation

Accordingly, we recommend that the Director of the Office of Management and Budget and the Assistant to the President for National

Security Affairs ensure that the various existing and newly initiated efforts to improve federal information security are coordinated under a comprehensive strategy. Such a strategy should

- ensure that executive agencies are carrying out the responsibilities outlined in laws and regulations requiring them to protect the security of their information resources;
- clearly delineate the roles of the various federal organizations with responsibilities related to federal information security;
- identify and rank the most significant information security issues facing federal agencies;
- promote information security risk awareness among senior agency officials whose critical operations rely on automated systems;
- identify and promote proven security tools, techniques, and management best practices;
- ensure the adequacy of information technology workforce skills;
- ensure that the security of both financial and nonfinancial systems is adequately evaluated on a regular basis;
- include long-term goals and objectives, including time frames, priorities, and annual performance goals; and
- provide for periodically evaluating agency performance from a governmentwide perspective and acting to address shortfalls.

Agency Comments and Our Evaluation

In commenting on a draft of this report, OMB's Acting Deputy Director for Management stated that OMB and the CIO Council, working with the National Security Council, have developed a plan to address the PDD 63 provision that the federal government serve as a model for critical infrastructure protection and to coordinate the new requirements of the PDD with the existing requirements of the various laws pertaining to federal information security. The comments further stated that the plan is to develop and promote a process by which government agencies can (1) identify and assess their existing security posture, (2) implement security best practices, and (3) set in motion a process of continued maintenance. Also described are plans for a CIO Council-sponsored interagency security assist team that will review agency security programs. Regarding our conclusion that many aspects of the recommendations in our September 1996 report are still applicable, OMB reiterated its concern that the 1996 report's "overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security."

OMB's comments indicate that it, the CIO Council, and the National Security Council are moving to coordinate their responsibilities and beginning to develop the comprehensive strategy that is needed. Based on the description provided, the plans being developed include several key elements, most notably a means of evaluating agency performance. These plans were still being finalized at the close of our work and were not yet available for our review. Accordingly, we are not able to comment on their content, scope, and detail, or whether they will be effective in improving federal information security.

Regarding OMB's concern that we have overemphasized its role, we agree that agency managers are primarily responsible for the security of their operations. Increased attention and support from central oversight, if done effectively, should not distract agencies from their responsibilities in this area. On the contrary, active oversight of agency performance is more likely to have the effect of emphasizing the agency managers' accountability and providing more visibility for agencies that are achieving their information assurance goals as well as those that are falling short.

Appendix I

GAO Reports on Information Security Issued Since March 1996

Note: This list does not include products for which distribution was limited to official use because the products contained sensitive information.

VA Information Systems: Computer Control Weaknesses Increase Risk of Fraud, Misuse and Improper Disclosure (GAO/AIMD-98-175, September 23, 1998).

FAA Systems: Serious Challenges Remain in Resolving Year 2000 and Computer Security Problems (GAO/T-AIMD-98-251, August 6, 1998).

Air Traffic Control: Weak Computer Security Practices Jeopardize Flight Safety (GAO/AIMD-98-155, May 18, 1998).

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

Executive Guide: Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68, May 1998).

U.S. Government Financial Statements: Results of GAO's Fiscal Year 1997 Audit (GAO/T-AIMD-98-128, April 1, 1998).

Financial Audit: Examination of IRS' Fiscal Year 1996 Custodial Financial Statements (GAO/AIMD-98-18, December 24, 1997).

Financial Management: Review of the Military Retirement Trust Fund's Actuarial Model and Related Computer Controls (GAO/AIMD-97-128, September 9, 1997).

Financial Audit: Examination of IRS' Fiscal Year 1996 Administrative Financial Statements (GAO/AIMD-97-89, August 29, 1997).

Small Business Administration: Better Planning and Controls Needed for Information Systems (GAO/AIMD-97-94, June 27, 1997).

Social Security Administration: Internet Access to Personal Earnings and Benefits Information (GAO/T-AIMD/HEHS-97-123, May 6, 1997).

Budget Process: Comments on S.261—Biennial Budgeting and Appropriations Act (GAO/T-AIMD-97-84, April 23, 1997).

IRS Systems Security and Funding: Employee Browsing Not Being Addressed Effectively and Budget Requests for New Systems Development Not Justified (GAO/T-AIMD-97-82, April 15, 1997).

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/T-AIMD-97-76, April 10, 1997).

IRS Systems Security: Tax Processing Operations and Data Still at Risk Due to Serious Weaknesses (GAO/AIMD-97-49, April 8, 1997).

High Risk Series: Information Management and Technology (GAO/HR-97-9, February 1997).

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

Financial Audit: Examination of IRS' Fiscal Year 1995 Financial Statements (GAO/AIMD-96-101, July 11, 1996).

Tax Systems Modernization: Actions Underway But IRS Has Not Yet Corrected Management and Technical Weaknesses (GAO/AIMD-96-106, June 7, 1996).

Information Security: Computer Hacker Information Available on the Internet (GAO/T-AIMD-96-108, June 5, 1996).

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/AIMD-96-84, May 22, 1996).

Information Security: Computer Attacks at Department of Defense Pose Increasing Risks (GAO/T-AIMD-96-92, May 22, 1996).

Security Weaknesses at IRS' Cyberfile Data Center (GAO/AIMD-96-85R, May 9, 1996).

Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996).

Appendix II

Agency Reports Issued Since September 1996 That Identify Information Security Weaknesses

Department of Health and Human Services Accountability Report: Fiscal Year 1997 (April 1998).

Report on the Financial Statement Audit of the Health Care Financing Administration for Fiscal Year 1997 (A-17-97-00097, April 24, 1998).

Report on the Department of Health and Human Services Consolidated Financial Statements for Fiscal Year 1997 (A-17-98-00001, April 1, 1998).

Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1997 and 1996 Financial Statements (OIG-98-050, March 5, 1998).

Audit of the Extent to Which USAID's Financial Management System Meets Requirements Identified in the Federal Financial Management Improvement Act of 1996 (OIG-A-000-98-003-P, March 2, 1998).

Report on USAID's Financial Statements, Internal Controls, and Compliance for Fiscal Years 1997 and 1996 (OIG-0-000-98-001-F, March 2, 1998).

EPA's Fiscal Year 1997 and 1996 Financial Statements Audit Report (E1AML7-20-7008-8100058, March 2, 1998).

NASA Data Center General Controls, Johnson Space Center (IG-98-005, January 29, 1998).

Federal Managers' Financial Integrity Act Report, Fiscal Year 1997 (USAID, December 31, 1997).

EPA 1997 Integrity Act Report to the President and Congress (EPA-205-R-98-002, December 19, 1997).

Social Security Accountability Report for Fiscal Year 1997, (SSA Pub. No. 31-231, November 1997).

General and Application Controls Over the Mechanization of Contract Administration Services System (DODIG, Report Number 98-007, October 9, 1997).

Audit of USAID's Compliance with Federal Computer Security Requirements (OIG-A-000-97-008-P, September 30, 1997).

Audit of the Status of USAID's New Management System (NMS) (OIG-A-000-97-010-P, September 30, 1997).

Audit of the Internal Controls for the Operational New Management System (OIG-A-000-97-009-P, September 30, 1997).

NASA Data Center General Controls, Marshall Space Flight Center (IG-97-039, September 30, 1997).

Evaluation of the Social Security Administration's Back-up and Recovery Testing of Its Automated Systems (SSA/OIG-A-13-97-12014, September 24, 1997).

U.S. Department of Justice Annual Financial Statement for Fiscal Year 1996 (DOJ/OIG-97-24B, September 1997).

Report on the Financial Statement Audit of the Department of Health and Human Services for Fiscal Year 1996 (A-17-96-0001, August 29, 1997).

NASA Data Center Facility, Langley Research Center (IG-97-035, August 28, 1997).

U.S. Department of Education Fiscal Years 1996 and 1995 Financial Statements and Accompanying Notes (Price Waterhouse, LLP, July 31, 1997).

Physical Security at Ames Research Center's NAS Facility (IG-97-030, July 18, 1997).

Audit of USAID's Efforts to Resolve the Year 2000 Problem (OIG-A-000-97-005-P, July 11, 1997).

Department of the Treasury's Inspector General Report: Audit of the Bureau of Alcohol, Tobacco and Firearms Fiscal Years 1996 and 1995 Financial Statements (OIG-97-094, July 9, 1997).

The Royalty Management Program's Automated Information Systems, Minerals Management Service (DOI/OIG-97-I-1042, July 1997).

Review of Physical Security at the Social Security Administration's National Computer Center (SSA/OIG-A-13-96-11046, June 26, 1997).

Audit of OPM's Benefit Programs Fiscal Year 1996 Financial Statements - Management Letter (Transmitted to OPM's OIG on June 20, 1997).

Review of the Back-up and Recovery Procedures at the National Computer Center (SSA/OIG-A-13-96-11052, June 19, 1997).

Audit of OPM's Benefit Programs Fiscal Year 1996 Financial Statements (Transmitted to the Director, OPM, on June 17, 1997).

General Services Administration, Fiscal Year 1996 Management Letter Comments and Suggestions for Consideration (OIG-A62709, June 10, 1997).

Audit of Security Controls at the Hines Benefits Delivery Center, Department of Veterans Affairs, Office of Inspector General (Report Number 7D2-G07-062, May 13, 1997).

Audit of SBA's FY 1996 Financial Statements - Management Letter (SBA/OIG-7-6-H-006-015, April 29, 1997).

Audit of the U.S. Department of Housing and Urban Development's Fiscal Year 1996 Financial Statements (Case Number 97-FO-177-0003, April 10, 1997).

Report on the Department of Transportation Fiscal Year 1996 Consolidated Financial Statement (Report Number AD-OT-7-004, April 10, 1997).

Federal Emergency Management Agency Management Letter for the Year Ended September 30, 1996 (April 4, 1997).

General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (DOI/OIG-97-I-771, April 1997).

Department of the Treasury's Inspector General Report: Report on the U.S. Customs Service's Fiscal Years 1996 and 1995 Financial Statements (OIG-97-054, March 31, 1997).

NSF's Fiscal Year 1996 Management Letter Report (OIG-97-2110, March 31, 1997).

Review of CA-TOP SECRET Access Control Software (SSA/OIG-A-13-95-00606, March 18, 1997).

Department of Commerce's Consolidating Financial Statements for Fiscal Year 1996 (OIG-FSD-9355-7-0001, March 1, 1997).

Department of Commerce Economic Development Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8837-7-0001, March 1, 1997).

Department of Commerce International Trade Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8838-7-0001, March 1, 1997).

Department of Commerce National Oceanic and Atmospheric Administration Financial Statements for Fiscal Year 1996 (OIG-FSC-8841-7-0001, March 1, 1997).

Mainframe Computer Policies and Procedures, Administrative Service Center, Bureau of Reclamation (DOI/OIG-97-I-683, March 1997).

U.S. Environmental Protection Agency FY 1996 Audited Financial Statements (March 1997).

Audit of SBA's FY 1996 Financial Statements (SBA/OIG-7-6-H-006-010, February 28, 1997).

Auditor's Reports on NSF's Fiscal Year 1996 Financial Statements, (Transmitted to the Chairman, NSF, on February 28, 1997).

U.S. Department of Labor Consolidated Financial Statement Audit for Fiscal Years 1995 and 1996 (DOL/OIG-12-97-005-13-001, February 28, 1997).

Reports on USAID's Financial Statements, Internal Controls, and Compliance for Fiscal Year 1996 (OIG-0-000-97-001-C, February 24, 1997).

Department of Veterans Affairs Annual Accountability Report for Fiscal Year 1996 (February 14, 1997).

U.S. Department of Energy Consolidated Financial Statements for Fiscal Year 1996 (February 1997).

Management Letter to the Administrator of NASA (January 31, 1997).

Secretary's Annual Statement and Report, Federal Managers' Financial Integrity Act, U.S. Department of the Treasury 1996 (December 30, 1996).

Report on Applying Agreed-Upon Procedures to the Internal Controls over the Federal Financial System, Fiscal Year Ended September 30, 1996 (NRC/OIG, November 25, 1996).

General Control Environment of the Federal Financial System at the Reston General Purpose Computer Center, U. S. Geological Survey (DOI/OIG-97-I-98, October 1996).

Interim Report on the Status of USAID's New Management System (OIG-A-000-96-001-S, September 27, 1996).

Department of Health and Human Services Accountability Report: Fiscal Year 1996.

Department of State Consolidated Financial Statements for Fiscal Year 1996.

Financial Statements Fiscal Year 1996, Office of Personnel Management.

National Aeronautics and Space Administration Fiscal Year 1996 Accountability Report.

Appendix III

Comments From the Office of Management and Budget

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

September 14, 1998

The Honorable Gene L. Dodaro
Assistant Comptroller General
U.S. General Accounting Office
Washington, DC 20548

Dear Mr. Dodaro:

Thank you for the opportunity to comment on your draft report entitled, Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk (GAO/AIMD-98-92). The report's principal findings highlight many of the security challenges that are facing Federal agencies and other organizations as they increasingly rely on interconnected information systems for the conduct of agency business. The Office of Management and Budget (OMB) and the CIO Council have recognized these challenges, and, as the report acknowledges, have undertaken a number of initiatives to address them. The draft report also highlights the requirements of Presidential Decision Directive 63 which requires, among other things, that the Federal government serve as a model for critical infrastructure protection.

OMB and the CIO Council, working with the National Security Council, have developed a plan to address that charge and coordinate the new requirements of the PDD with the existing requirements of the Computer Security Act, Paperwork Reduction Act, and Clinger-Cohen Act. Our plan, which is integrated with the CIO Council Security Committee's strategic plan, is to develop and promote a process by which government agencies can: 1) identify and assess their existing security posture; 2) implement security best practices to assure program improvement and effectiveness; and, 3) set in motion a process of continued maintenance. Coordination of these efforts will come primarily from the CIO Council and the President's Management Council, both co-chaired by OMB.

As part of this process, the CIO Council will sponsor an inter-agency security assist team that will perform independent and confidential reviews of agency security programs. As agency needs dictate, these reviews will include top-level program reviews for conformance to OMB Circular A-130, Appendix III and GAO's executive guide, "Information Security Management: Learning from Leading Organizations," and system-specific reviews to evaluate conformance with the Computer Security Handbook issued by the National Institute of Standards and Technology . Each review will also include selective system interdependency analysis and penetration testing. As GAO has found, among the chief benefits of penetration testing is the way it vividly demonstrates to agency managers the inadequacies of seemingly secure systems and programs.

The greatest challenge to enhancing information security programs and developing a workable infrastructure protection program is to ensure that protection efforts are "owned" by the program and business managers at the agencies who are accountable for the success of their entire program, including security. This essential aspect was underscored in GAO's Executive Guide. By working through the CIO Council and the President's Management Council, we will be able to improve coordination of security requirements and link security measures to business risks and agency mission. In this way security programs will support, not restrict, mission accomplishment.

The draft report also states that while federal information security has received increased visibility and attention since September 1996, central oversight remains limited and a comprehensive strategy has not been developed. The draft thus concludes that many aspects of the recommendations made in GAO's 1996 report, "Information Security: Opportunities for Improved OMB Oversight of Agency Practices (GAO/AIMD-96-110) remain applicable. We reiterate in part the response we made at that time, i.e., "The central thrust of the ITMRA is to increase the authority, responsibility, and accountability of Federal agencies for the management of their information resources. Ultimately we are concerned that the report's overemphasis on OMB's role could distract program managers in the Federal agencies from their primary responsibility for assuring information security."

On the draft report's recommendation to OMB and the NSC that the "various existing and newly initiated [via PDD-63] efforts to improve federal information security are coordinated under a comprehensive strategy," we are confident that the CIO Council's strategic plan as well as the plan of the Council's security committee along with the efforts we have described above address that recommendation.

Sincerely,

G. Edward DeSeve

G. Edward DeSeve
Acting Deputy Director
for Management

Appendix IV

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.	Jean H. Boltz, Assistant Director, (202) 512-5247 Ronald W. Beers, Assistant Director Darrell L. Heim, Assistant Director Carol A. Langelier, Assistant Director Crawford L. Thompson, Assistant Director Gregory C. Wilshusen, Assistant Director Gary R. Austin, Senior Information Systems Analyst Kirk J. Daubenspeck, Senior Information Systems Analyst Ernest A. Döring, Senior Evaluator Michael W. Gilmore, Senior Information Systems Analyst William F. Wadsworth, Senior Information Systems Analyst
Atlanta Field Office	Sharon S. Kittrell, Senior EDP Auditor
Dallas Field Office	David W. Irvin, Assistant Director Debra M. Conner, Senior EDP Auditor Shannon Q. Cross, Senior Evaluator William H. Thompson, Senior Evaluator Charles M. Vrabel, Senior EDP Auditor

ISBN 0-16-057920-1