CRITICAL INFRASTRUCTURE PROTECTION

Comprehensive Strategy Can Draw on Year 2000 Experiences
# Contents

## Letter

3

## Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appendix I</td>
<td>Objectives, Scope, and Methodology</td>
<td>30</td>
</tr>
<tr>
<td>Appendix II</td>
<td>GAO Reports and Testimonies Addressing Information Security Issues Since February 1996</td>
<td>32</td>
</tr>
<tr>
<td>Appendix III</td>
<td>GAO Reports and Testimonies Addressing the Year 2000 Challenge</td>
<td>36</td>
</tr>
<tr>
<td>Appendix IV</td>
<td>Risks to Computer-Supported Operations</td>
<td>48</td>
</tr>
<tr>
<td>Appendix V</td>
<td>Examples of Information Security Weaknesses Reported by GAO for Federal Agencies During Fiscal Year 1999</td>
<td>50</td>
</tr>
</tbody>
</table>

## Figure

7

## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>DOD</td>
<td>Department of Defense</td>
</tr>
<tr>
<td>FBI</td>
<td>Federal Bureau of Investigation</td>
</tr>
<tr>
<td>FISCAM</td>
<td>Federal Information System Controls Audit Manual</td>
</tr>
<tr>
<td>ICC</td>
<td>Information Coordination Center</td>
</tr>
<tr>
<td>NASA</td>
<td>National Aeronautics and Space Administration</td>
</tr>
<tr>
<td>NCS</td>
<td>National Communications Systems</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NIPC</td>
<td>National Infrastructure Protection Center</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency</td>
</tr>
<tr>
<td>OMB</td>
<td>Office of Management and Budget</td>
</tr>
<tr>
<td>OPM</td>
<td>Office of Personnel Management</td>
</tr>
<tr>
<td>PDD</td>
<td>Presidential Decision Directive</td>
</tr>
</tbody>
</table>
October 1, 1999

The Honorable Robert F. Bennett
Chairman
Special Committee on the Year 2000 Technology Problem
United States Senate

Dear Mr. Chairman:

Since the early 1990s, an explosion in computer interconnectivity, most notably growth in use of the Internet, has revolutionized the way our government, our nation, and much of the world communicate and conduct business. The benefits have been enormous. Vast amounts of information are now literally at our fingertips, facilitating research on virtually every topic imaginable; financial and other business transactions can be executed almost instantaneously, often on a 24-hour-a-day basis; and electronic mail, Internet websites, and computer bulletin boards allow us to communicate quickly and easily with a virtually unlimited number of other individuals and groups. However, in addition to its benefits, this widespread interconnectivity poses enormous risks to our computer systems and, more importantly, to the critical operations and infrastructures they support, such as telecommunications; power distribution; national defense, including the military's warfighting capability; law enforcement; government services; and emergency services.

Recent efforts to address the Year 2000 computing problem have called attention to some important aspects of these risks. In particular, the Year 2000 problem has highlighted computer-based interdependencies and the vulnerability of these systems to disruption. It also has underscored the need to develop awareness, cooperation, and a disciplined management approach to adequately address such problems. In many ways, the Year 2000 challenge can be viewed as a major test of our nation's ability to protect its computer-supported critical infrastructures; although, protecting critical infrastructures from hostile attacks on a continuous basis will require addressing a much broader array of issues.

This report responds to your request that we (1) summarize our recent findings on computer security and critical infrastructure protection and (2) identify preliminary lessons learned from the Year 2000 date conversion
experience that can benefit critical infrastructure protection efforts. It is based both on reports we issued during 1997 and 1998 and the first 9 months of 1999 and on recent discussions with key officials involved in the Year 2000 conversion efforts and critical infrastructure protection. Appendix I contains a more detailed description of our objectives, scope, and methodology. Appendix II lists our reports and testimonies that address information security, and appendix III lists our reports and testimonies that address the Year 2000 challenge.

Results in Brief

Our nation’s computer-based critical infrastructures are at increasing risk of severe disruption. Interconnectivity increases the risk that problems affecting one system will also affect other interconnected systems. Massive computer networks provide pathways among systems that, if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as earthquakes, and system-induced problems, such as the Year 2000 date conversion problem, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

The resultant damage can vary, depending on the threat. Critical system operations can be disrupted or otherwise sabotaged, sensitive data can be read and copied, and data or processes can be tampered with. A significant concern is that terrorists or hostile foreign states could launch computer-based attacks on critical systems, such as those supporting energy distribution, telecommunications, and financial services, to severely damage or disrupt our national defense or other operations, resulting in harm to the public welfare. Understanding these risks to our computer-based critical infrastructures and determining how best to mitigate them are major information security challenges.
The need to strengthen computer security in both government and the private sector has been recognized over the past few years by a number of entities, and several initial steps have been taken to address the problem. Since 1994, we have issued dozens of reports on individual agency computer security weaknesses and made scores of related recommendations. In September 1996, we reported that poor information security was a widespread federal problem. ¹ Subsequently, in February 1997, in a series of reports to the Congress, we designated information security as a new governmentwide high-risk area. ²

During 1996 and 1997, federal information security 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. These efforts were supplemented in late 1997 when the federal Chief Information Officers (CIO) Council designated information security as one of six priority areas and established a Security Committee, which has taken steps to promote awareness, improve agency access to incident response services, and support agency improvement efforts.

In May 1998, Presidential Decision Directive (PDD) 63 recognized that addressing computer-based risks to our nation's critical infrastructures requires a new approach that involves coordination and cooperation across federal agencies and among public and private-sector entities and other nations. PDD 63 created several new entities for developing and implementing a strategy for critical infrastructure protection. In addition, it tasked federal agencies with developing critical infrastructure protection plans and establishing related links with private industry sectors. Since then, a variety of activities have been undertaken, including development and review of individual agency's critical infrastructure protection plans, identification and evaluation of information security standards and best practices, and efforts to build communication links with the private sector. However, the details of an approach for implementing PDD 63 are still


being developed. In particular, the first version of a key element called for in PDD 63—development of a national plan for critical infrastructure protection—has not been completed. As a result, it is not clear how the activities undertaken to date interrelate and whether they will effectively and efficiently support national goals. As of late August, those involved in developing the plan expected it to be issued in late October of this year.

As the plan is finalized and discussed, a number of issues will need to be resolved, including those regarding the federal government's role in critical infrastructure protection and how best to balance potentially competing demands for security versus privacy. Many of these issues are different from those associated with the Year 2000 challenge. However, it is important that our government take advantage of the experience it has gained and is continuing to gain in addressing the Year 2000 challenge as it strives to reduce the risk associated with longer-term threats to our critical infrastructures. Although it is too early to identify a comprehensive set of lessons learned, some factors provide preliminary insights into the challenge ahead. In particular, the Year 2000 experience has provided a foundation for improvement and has already clearly shown the value of

- high-level congressional and executive branch leadership,
- understanding risks to computer-supported operations,
- providing adequate technical expertise,
- providing standard guidance,
- establishing public-private sector relationships,
- facilitating progress and monitoring performance,
- developing an incident identification and coordination capability, and
- implementing fundamental information technology management improvements.

Risks to Computer-Dependent Operations Are Substantial

The risks associated with our nation's reliance on interconnected computer systems are substantial and varied. The Year 2000 challenge has vividly illustrated the risks posed by a widespread system-induced computing problem. However, numerous other threats will continue to pose risks long after the Year 2000 problem has been resolved. Some, similar to the Year 2000 problem, could cause severe disruption, while others more directly threaten the confidentiality or integrity of data. The following diagram provides an overview of the various types of risks. A more detailed description, based on a list compiled by the National Institute of Standards and Technology (NIST), is in appendix IV.
Figure 1: Risks to Computer-Based Operations

- **Threats**
  - Hostile States
  - Spies/Snoops
  - Saboteurs
  - Terrorists
  - Natural Disasters
  - User Error
  - Fraud
  - Pranksters
  - Criminals

- **Potential Damage**
  - Critical Operations Halted
  - Services & Benefits Interrupted
  - Assets Lost
  - Integrity of Data & Reports Corrupted
  - Sensitive Data Disclosed
  - Consumer & Taxpayer Confidence Lost
  - Integrity of Data & Reports Corrupted
  - Assets Lost
  - Services & Benefits Interrupted
  - Sensitive Data Disclosed
  - Consumer & Taxpayer Confidence Lost
While complete summary data are not available because many computer security incidents are not reported, the number of incidents is clearly growing. For example, the number of reported incidents handled by Carnegie-Mellon University's CERT Coordination Center\(^3\) has increased from 1,334 in 1993 to 4,398 during the first two quarters of 1999. Similarly, the fourth annual survey conducted by the Computer Security Institute in cooperation with the Federal Bureau of Investigation (FBI) showed an increase in computer system intrusions for the third year in a row. In 1999, 30 percent of 521 respondents from both the private and public sectors reported such attacks.\(^4\)

Many incidents appear to be unrelated and result in relatively limited damage. However, a widespread, well-organized attack could severely disrupt or damage critical systems that are essential to our national defense, economic prosperity, and quality of life.

In the federal government, these risks are not being adequately addressed. Tests and evaluations of federal systems show that these systems are not being effectively protected, even though they process, store, and transmit enormous amounts of sensitive data and are indispensable to many federal agency operations.

Even greater concerns have been raised about the security of private sector systems, which control most of our nation's critical infrastructures, such as energy, telecommunications, financial services, transportation, and vital human services. Virtually all U.S. residents and businesses rely on these infrastructures, including government operations. One cause of concern is that although there are numerous reports of individual system intrusions and failures, there is little summary information that can be used to more accurately estimate the risk. Few reports are publicly available about the effectiveness of controls over privately controlled systems, and private entities are reluctant to disclose known problems or vulnerabilities that

\(^{3}\text{Originally called the Computer Emergency Response Team, the center was established in 1988 by the Defense Advanced Research Projects Agency. It is charged with (1) establishing a capability to quickly and effectively coordinate communication among experts in order to limit the damage associated with, and respond to, incidents and (2) building awareness of security issues across the Internet community.}\)

might weaken their competitive positions or diminish customer confidence in their services or products.

In order to determine adequate levels of protection to safeguard our critical infrastructures, it will be important to gain a more thorough understanding of the related risks. This will be an ongoing effort due to fast-paced changes in computer technology and in the tools and techniques available to would-be intruders. As these risks are assessed, it will be important to consider that the computer security improvements that would guard against purposeful, hostile attacks on critical infrastructures could also provide other benefits that would allow our nation and others to take further advantage of computer technology. In particular, improved security would provide businesses and individuals greater confidence in the integrity and confidentiality of computerized information. Such confidence would be likely to increase people's willingness to engage in electronic commerce and have confidential data, such as financial and medical records, maintained and transmitted electronically.

**Risks to Federal Operations**

Federal operations, such as national defense, tax collection, law enforcement, air traffic control, and benefit payments are at risk of disruption, as well as fraud and inappropriate disclosures, due to a variety of security weaknesses associated with the computers on which such operations depend. Organized attacks, such as the "Solar Sunrise" attack on Department of Defense (DOD) and other computers in early 1998, and widespread computer virus infections, such as the Melissa virus in early 1999, illustrate our government's susceptibility to malicious computer-based actions.

According to the DOD, Solar Sunrise was a series of attacks during February 1998 that targeted its servers by exploiting a well-known vulnerability in the Solaris operating system. The attacks were widespread and systematic and showed a pattern that indicated they might be the preparation for a coordinated attack on DOD's information infrastructure. They were of particular concern because they targeted key parts of DOD's networks at a time when it was preparing for possible military operations against Iraq. As we testified in April 1999, the Melissa virus affected Microsoft word processing software. Although the Melissa virus disrupted

---

operations at thousands of companies and some government agencies, it reportedly did not compromise sensitive government data. However, it illustrated the speed with which malicious software can spread in today’s interconnected computing environment.

Audit reports we and agency inspectors general issued during fiscal year 1999 show that 22 of the largest federal agencies have significant computer security weaknesses—which closely mirrors a finding we reported in September 1998.6 Reports we issued during the past year describe risks to operations and assets at the National Aeronautics and Space Administration and the Departments of Defense, Agriculture, and Treasury. Appendix V provides more detailed descriptions of these weaknesses.

These recent reports supplement a body of evidence on federal computer security problems at individual agencies that we have compiled since 1996. These reports have provided scores of recommendations for improvement. In addition, we have issued several summary reports that provide a more comprehensive view of the problem and illustrate the need for concerted improvement efforts.

- In September 1996, we reported that since September 1994, serious weaknesses had been reported for 10 of the largest 15 federal agencies.7 In that report we concluded that poor information security was a widespread federal problem with potentially devastating consequences, and we recommended that the Office of Management and Budget (OMB) play a more proactive role in overseeing agency practices and managing improvements.
- In February 1997 and again in January 1999, our reports to the Congress designated information security as a governmentwide high-risk area.8

• In our March 1998 and March 1999 reports on the federal government’s consolidated financial statements, we reported that widespread and serious computer control 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.9

• In September 1998, we reported that critical federal operations were at risk of disruption, fraud, and inappropriate disclosure due to weaknesses in every major federal agency.10

In both our September 1996 and September 1998 reports and in testimony before the Senate Committee on Governmental Affairs in September 1998,11 we concluded that an underlying cause of weak information security at federal agencies was that agency officials had not instituted a basic cycle of management procedures for ensuring that risks are fully understood and that controls implemented to mitigate risks are effective.12 Our subsequent audits have continued to support this conclusion. In particular, many agencies are not adequately (1) assessing risks, (2) using the results of such assessments to select controls, (3) promoting awareness, (4) evaluating control effectiveness, and (5) coordinating their security program through a central agency focal point.

Our September 1996 and September 1998 reports also concluded that more effective actions were needed at the governmentwide level. In September 1998, we recognized efforts by OMB, NIST, the federal Chief Information Officers (CIO) Council, and the then newly initiated critical infrastructure protection efforts called for by PDD 63, but we also stated that a comprehensive governmentwide strategy was needed. We noted that the new entities and responsibilities prescribed by PDD 63 supplemented existing security requirements prescribed in the Paperwork Reduction Act of 1980, OMB Circular A-130, Appendix III, the Computer Security Act, the


12See footnotes 6 and 7, respectively.
Clinger-Cohen Act, and the Federal Managers’ Financial Integrity Act, as well as information security initiatives underway at organizations such as the CIO Council. We said that many of the existing organizations and those created by PDD 63 appeared to have overlapping objectives and that, accordingly, it was especially important that a governmentwide strategy be developed that clearly defined and coordinated the roles of new and existing federal entities in order to avoid inappropriate duplication of effort and ensure governmentwide cooperation and support.

Specifically, we recommended 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. We suggested that such a strategy

- 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 November 1998, key officials in OMB, the National Security Council, the FBI, the CIO Council, and the Year 2000 Office held a joint meeting and assured us that they were coordinating their efforts. Since then, we have observed many instances of cooperation and joint efforts. However, a strategy for improving federal information security has not yet been clearly articulated.
Broader Risks to Critical Infrastructures

While the federal government has traditionally focused on the security of its own systems, there has been a growing realization in recent years that our national welfare, including government services and national defense, depends to a large extent on systems supporting privately controlled infrastructures. This concern has been emphasized by the Year 2000 challenge as many agencies and private-sector organizations have been forced to recognize their dependence on computer systems beyond their span of control. Over the past few years, such risks and the need to adjust the way we view and protect our nation’s information systems have been described in a variety of reports and testimonies before the Congress. The following chronology provides an overview of this growing concern.

- A 1994 Joint Security Commission report warned that computer networks are “a battlefield of the future” and that the risk was not limited to military systems. According to the Commission, if an enemy attacked our unprotected civilian infrastructure (for example, the public telephone system), the economic and other results could be disastrous.\(^\text{13}\)

- In 1996, the Director of Central Intelligence stated that there is evidence that “a number of countries are developing the doctrine, strategies, and tools to conduct information attacks” and that “international terrorists groups clearly have the capability to attack the information infrastructure of the United States.” The Director’s greatest concern was that hackers, terrorists, or other nations could use information warfare techniques as part of a coordinated attack to seriously disrupt electric power distribution, air traffic control, or financial sectors.\(^\text{14}\)

- In October 1997, the President’s Commission on Critical Infrastructure Protection issued a comprehensive report on our nation’s computer-related vulnerabilities that described the potentially devastating implications of poor information security from a national perspective.\(^\text{15}\)


\(^{14}\)Statement for the Record by the Director of Central Intelligence to the U.S. Senate Committee on Governmental Affairs, Permanent Subcommittee on Investigations, “Foreign Information Warfare Programs and Capabilities,” June 25, 1996.

• In March 1998, the Chief of the National Infrastructure Protection Center (NIPC), Federal Bureau of Investigation, testified that “transnational criminals are rapidly becoming aware of and exploiting the power of cyber tools” and that recent computer crimes illustrate “the growing problem of cyber crime, the international dimension of the problem, and the increasing threat to our critical infrastructure.” According to the Chief, one example that illustrates the growing problem is the 1994 case where foreign crime groups hacked into a major financial service company’s cash management system and attempted transfers totaling $10 million.16

• In releasing a December 1998 report on “cyberwarfare” and crime prepared by a panel of current and former U.S. national security officials, former FBI and Central Intelligence Agency Director William Webster stated that “it is time for us to recognize that we have a range of enemies today, not only military enemies, but criminals and terrorists and others who have the same capabilities to do major damage to the infrastructure upon which we all depend.”17

• In May 1998, the President, through PDD 63, directed that a national plan on infrastructure protection be developed and addressed a range of other infrastructure protection issues.

• In June 1998 and in February 1999, the Director for Central Intelligence testified that several nations recognize that cyber attacks against civilian computer systems represent an option they could use to “level the playing field” during an armed crisis against the United States, and they are developing information warfare capabilities. He added that terrorists and others were beginning to recognize that information warfare offers them “low cost, easily hidden tools to support their causes.”18

16Statement for the Record, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, before the Congressional Joint Economic Committee, March 24, 1998.


18Testimony by Director for Central Intelligence before the Senate Committee on Governmental Affairs, June 24, 1998, and before the Senate Armed Services Committee, February 2, 1999.
In March 1999, the National Communications Systems (NCS), an interagency committee formed to examine communication networks and institute change, reported that adversaries could disrupt, disable, or collect sensitive data through coordinated attacks on U.S. computer systems and that organized crime groups are targeting such systems to commit fraud, acquire and exploit proprietary information, and steal funds and securities transmitted through electronic commerce systems.19

These reports and statements have focused attention on the issues associated with infrastructure protection, particularly vulnerabilities to critical operations and our national defense. They have also prompted the start of a national debate regarding the appropriate mix of public and private actions and types of mechanisms needed to better define and address these risks.

Critical Infrastructure Protection Requires a New Approach

As the President’s Commission on Critical Infrastructure Protection recognized in its October 1997 report, mitigating the shared risks resulting from our computer-based interdependencies will require shared, or jointly developed, solutions. Just as it is no longer satisfactory for individual organizations to address their computer security risks solely on a system-by-system basis, neither can individual organizations fully protect their operations without considering risks associated with systems they use or depend on that are controlled by others. Such systems can include those of business partners, public utilities, and government entities—in essence, any system on which an organization relies for essential services, information, or business transactions.

In response to the Commission’s report, the executive branch initiated efforts to implement a cooperative public-private approach to protecting our critical infrastructures by issuing PDD 63 in May 1998. PDD 63 calls for a range of actions intended to improve federal agency security programs, establish a partnership between the government and the private sector, and improve our nation’s ability to detect and respond to serious attacks. As described previously, to accomplish these goals, the directive (1) established a 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 and (2) created new entities within the Department of Commerce and the FBI. In addition, it assigned agencies new responsibilities for coordinating with industry sectors and developing critical infrastructure protection plans.

A central requirement of PDD 63 is development of a National Infrastructure Assurance Plan. As of late August 1999, officials involved in developing the plan estimated that it would be issued in late October 1999. Such a plan is important because it can provide a roadmap to guide the activities of the many federal entities involved in critical infrastructure protection. In particular the plan can provide for:

- defining and ranking risks to help ensure that attention and resources are focused on reducing the most significant vulnerabilities,
- designating roles and responsibilities,
- developing a plan of action for addressing the most significant risks first, and
- monitoring progress and measuring performance.

Defining and Ranking Risks

PDD 63 identified industry sectors and federal agencies that are important to critical infrastructure protection. However, a more detailed analysis is needed to determine the greatest specific risks, the most critical systems and interdependencies, and the improvement efforts that merit the earliest and greatest attention. Such an analysis and identification of risk needs to be done within individual organizations and agencies as well as across industry groups and government agencies in order to identify critical interdependencies. Without a prioritized lists of such factors, or a plan for developing such information, it will not be possible to determine what protective actions are needed and which should be undertaken first.

Designating Roles and Responsibilities

Many agencies have responsibilities related to computer security that overlap somewhat with new critical infrastructure protection initiatives. For example, under current laws, federal agencies are primarily responsible for adequately securing their own operations, OMB is responsible for overseeing and coordinating federal agency security, and NIST with assistance from the National Security Agency (NSA) is responsible for establishing related standards. In addition, since its establishment in 1996, the CIO Council has undertaken activities in this area. It is important that the roles of these organizations as they relate to
critical infrastructure protection be well defined and coordinated with those of newer entities established by PDD 63 within the National Security Council, the Department of Commerce, and the FBI.

Developing a Plan of Action

Once specific risks and interdependencies have been identified and ranked, an action plan can be developed to address them. To be most effective, such a plan should define specific objectives, estimate needed resources, and provide a schedule of activities.

During the 15 months since PDD 63’s issuance, a variety of activities have begun. Twenty-one federal agencies, identified as the most important to critical infrastructure protection, have submitted critical infrastructure protection plans and received at least one round of comments from an expert review team managed by the Critical Infrastructure Assurance Office, which was established by PDD 63 in the Department of Commerce. In addition, the General Services Administration, OMB, the CIO Council, NIST, and others have either engaged in cooperative efforts with the entities established by PDD 63 or reoriented or supplemented ongoing activities to support PDD 63 goals. Examples include the following:

• The CIO Council’s security committee created a sub-group for providing input on critical infrastructure protection efforts.
• The Critical Infrastructure Assurance Office is assisting in establishing the Information Coordination Center, which will monitor events surrounding January 1, 2000.
• NIST and NSA are leading an effort to identify and evaluate standards and best practices for information security.
• The FBI established the National Infrastructure Protection Center, in 1998, to facilitate and coordinate the federal government’s investigation and response to attacks on critical infrastructures.

However, these efforts are not yet being coordinated under a comprehensive plan. As a result, there is a risk that these efforts will be unfocused, inefficient, and ineffective. For example, the CIO Council Security Committee and a recently established working group both have efforts underway to identify standards and best practices that could improve federal agency efforts. While such efforts are generally laudable, it is unclear how the guidance that may result from them will relate to guidance issued by NIST and policies issued by OMB, two organizations that have statutory responsibilities in these areas.
Monitoring Progress and Measuring Performance

Once a plan of action has been developed and agreed on, it must be implemented. Ensuring effective implementation will require monitoring and evaluation to determine if milestones are being met and testing to determine if measures to protect critical infrastructures are operating as intended.

Evaluations at several levels can be beneficial. A program to periodically test and evaluate agency controls would provide agency managers with the information they need to determine if controls are operating effectively on an ongoing basis and whether adjustments to agency policies and procedures are needed. Evaluations by agency inspectors general or outside auditors can serve as an independent check on management evaluations. However, the emphasis should be on evaluations initiated by management, since computer security is a fundamental, ongoing management responsibility. Summary evaluations performed by entities such as OMB, GAO, or the CIO Council can provide a governmentwide view of progress and help identify crosscutting problems.

Year 2000 Efforts Provide Important Insights for Critical Infrastructure Protection

While the challenge of protecting our critical infrastructures is different in many ways from addressing the Year 2000 challenge, there are significant similarities. Critical infrastructure protection will raise many issues beyond those raised in addressing the Year 2000 problem, such as those pertaining to the role of government in ensuring protection of privately controlled infrastructures and how best to balance security needs with business and individual privacy. However, both challenges involve threats to critical computer-dependent operations, and both require actions by and cooperation among public and private sector entities.

While it is too early to comprehensively identify lessons learned from the Year 2000 conversion efforts, we identified a number of factors from the Year 2000 experience that are relevant to longer term critical infrastructure protection and provide insights into the challenges ahead. In some areas, the Year 2000 problem has laid a foundation for longer term improvements in the way we view, manage, and protect computer systems supporting our nation's critical infrastructures. These areas include:

- providing high-level congressional and executive branch leadership,
- understanding risks to computer-supported operations,
- providing adequate technical expertise,
- providing standard guidance,
• establishing public-private sector relationships,
• facilitating progress and monitoring performance,
• developing an incident identification and coordination capability, and
• implementing fundamental information technology management improvements.

These factors, which are discussed below, should be considered when developing a national strategy for critical infrastructure protection.

Providing Congressional and Executive Branch Leadership

One of the most important factors in prompting attention and action on the Year 2000 problem has been proactive leadership at the highest levels of government. In February 1998, the President signed an executive order establishing the President's Council on Year 2000 Conversion, chaired by an Assistant to the President and consisting of one representative from each of the executive departments and from other federal agencies as may be determined by the chair. The Council has focused attention on the problem and provided a forum for high-level communication among leaders in government, the private sector, and the international community. A similar entity, the Critical Infrastructure Coordination Group, was established by PDD 63. However, as yet, it has not had the same level of visibility as the Council on Year 2000 Conversion or as broad a level of agency participation.

In addition to executive branch leadership, congressional leadership has been important in addressing the Year 2000 challenge and can serve as a model for long-term critical infrastructure protection. The Senate formed a Special Committee on the Year 2000 Technology Problem, which held numerous hearings on the readiness of key economic sectors, including power, health care, telecommunications, transportation, financial services, emergency services, and general business. Similarly, the House called on the Subcommittee on Government Management, Information and Technology of the Committee on Government Reform and the Subcommittee on Technology of the Committee on Science to co-chair the House's Year 2000 monitoring. These and other congressional committees and subcommittees have played a central role in addressing the Year 2000 challenge by holding agencies accountable for demonstrating progress and by heightening public appreciation of the problem.

Understanding Risks

According to officials involved in Year 2000 conversion efforts, the Year 2000 challenge has served as a wake-up call to many who were previously
unaware of our nation's extensive dependency on computers. This new awareness of the importance of computer systems and of the vulnerabilities of these systems can serve as a basis for better understanding long-term risks to computer-supported critical infrastructures. In addition, Year 2000 efforts have forced agencies to identify those systems that are mission-critical.

At the governmentwide level, OMB identified 43 high-impact programs and designated a lead agency for each program. Each lead agency was directed to identify the partners integral to program delivery and take a lead role in convening those partners and ensuring that they had adequate Year 2000 plans. For those without plans, agencies were to help develop a plan to ensure that the related program would operate effectively.

These are important first steps for critical infrastructure protection because they provide organizations, industry groups, and government sectors a basis for helping to ensure that their most significant risks are addressed first. However, unlike the Year 2000 problem, critical infrastructure protection will be an ongoing challenge. Because risks and related system priorities change over time, as do the techniques for mitigating risks, infrastructure protection will require organizations to institutionalize the practices of inventorying and prioritizing their systems through periodic risk assessments. Our recent study of information security risk assessment practices at leading organizations provides guidance that agencies can use to develop a practical risk assessment program.20

Providing Adequate Technical Expertise

In April 1998, we noted that some agencies were reporting problems obtaining and retaining personnel with the technical expertise needed to accomplish Year 2000 conversions. Accordingly, we recommended that the Council for Year 2000 Conversion develop a personnel strategy that would include reemploying former federal employees and identifying ways to retain key Year 2000 staff. In October 1998, we reported that several efforts had been undertaken to address these workforce issues. Some of these illustrate the types of creative solutions that can be considered to solve specific personnel problems. Others serve as a basis for further improvements that could benefit critical infrastructure protection, as well as other information technology management issues.

To address information technology workforce shortages that agencies said were impeding their ability to make Year 2000 conversions, the Office of Personnel Management (OPM) publicized existing tools for retaining staff and supplemented these with additional aids. The tools that were publicized included:

- providing authority to reemploy federal retirees to work specifically on the Year 2000 conversion without the usually required reduction in the retiree's salary or military annuity;
- encouraging agency heads to exercise their authority to make exceptions to limitations on premium pay (including overtime, night, and holiday pay) for employees performing emergency work to resolve computer system problems associated with the Year 2000 that posed a direct threat to life and property;
- allowing agencies, in certain circumstances and with OPM approval, to exclude critical Year 2000 positions from voluntary early retirement programs; and
- allowing agencies to authorize a retention allowance of up to 10 percent of an employee's rate of basic pay (or up to 25 percent with OPM approval) for a group or category of employees such as computer programmers and system engineers that meet certain criteria, such as being likely to leave federal service in the absence of the allowance.


In addition, as we reported in October 1998, the Year 2000 Conversion Council took several steps to address personnel shortages from a nationwide perspective. These included (1) establishing an Internet site to link information technology workers with the companies that need them to solve the Year 2000 problem and (2) surveying community colleges to determine the effect of workforce issues on local communities.

Perhaps most importantly for the long term and prompted in part by concerns over technical staff shortages affecting Year 2000 efforts, the CIO Council, in March 1998, tasked its Education and Training committee with crafting recommendations for actions to help agencies recruit and retain information technology personnel. The final report was issued in June 1999, generally too late to provide substantive support for the Year 2000 efforts. However, the report provides an extensive description of the current status of federal information technology employment, improvement efforts currently underway, and detailed proposals for action that are associated with 13 major recommendations. In this regard, the report provides a useful basis for improving the federal information technology workforce as a whole, including that segment needed to support critical infrastructure protection efforts.

Providing Standard Guidance

Standard guidance that was universally accepted, adopted, and implemented has facilitated Year 2000 conversion efforts and related oversight. In particular, guidance issued from 1997 through 1999 by GAO, OMB, and the CIO Council has

- provided a level of consistency across government by providing standard terms, tools, and techniques based on best practices;
- imposed structure and discipline;
- increased the rigor of testing and assessment efforts;
- promoted consistency in data gathering and reporting; and
- facilitated audit and evaluation efforts by both agency management and auditors.
To help agencies mitigate their Year 2000 risks, we produced a series of Year 2000 guides that were adopted by OMB. The first of these, on enterprise readiness, provides a systematic, step-by-step approach for agency planning and management of its Year 2000 program. The second, on business continuity and contingency planning, provides a structured approach to helping agencies ensure minimum levels of service through proper planning. Our third guide sets forth a disciplined approach to Year 2000 testing. Federal agencies and other organizations have used these guides extensively to help organize and manage their Year 2000 programs. In addition, an interagency working group (which later evolved into the CIO Council's Year 2000 Committee) developed a best practices guide for Year 2000 conversion and made it available on the World Wide Web.

Similar guides could be developed for critical infrastructure protection. These could be based to a large extent on existing guides pertaining to various aspects of computer security. For example, since May 1998, we have issued two guides on information security management and risk assessment practices that can be applied to critical infrastructure protection as well as a broader range of information security risks.

In addition, since May 1997, OMB has provided agencies with instructions on reporting on their quarterly Year 2000 progress. These instructions covered items such as Year 2000 remediation progress, data exchanges, and costs. OMB periodically updated these instructions to request that agencies provide additional information on key topics such as verification actions or to clarify existing reporting requirements.

Establishing Public-Private Sector Relationships

Like the Year 2000 problem, the challenge of protecting critical infrastructures from computer-based attacks extends well beyond federal operations. It spans the entire spectrum of our national, as well as the global, economy. Many critical infrastructure facilities are owned and operated by private companies whose continued secure operations are

---


essential to the national welfare—as well as government services. As a result, establishing public-private partnerships has been recognized as one of the major challenges of critical infrastructure protection.

The Year 2000 challenge has provided a basis on which to build by establishing relationships that can serve as the beginning of such partnerships. It was essential that Year 2000 issues be adequately addressed in arenas beyond the federal government: state and local governments, the public infrastructure, and other key economic sectors, such as financial services. This is because a single failure in one system could affect many others in our nation’s complex array of public and private enterprises that have scores of system interdependencies at all levels.

To address these concerns, we recommended in April 1998 that the President’s Council on Year 2000 Conversion use a sector-based approach and establish the effective public-private partnerships necessary to address this issue. The Council subsequently established over 25 sector-based working groups and has been initiating outreach activities since it became operational in Spring 1998. Similar sectors and agency focal points were designated by PDD 63.

In addition, the Chair of the President’s Council has formed a Senior Advisors Group composed of representatives from private-sector firms across key economic sectors. Members of this group are expected to offer perspectives on crosscutting issues, information sharing, and appropriate federal responses to potential Year 2000 failures. In July 1999, the President directed establishment of a similar advisory group for critical infrastructure protection. The National Infrastructure Assurance Council, authorized by Executive Order 13130, is to have 30 members from private industry who are expected to be designated by late 1999. This new Council is to “support a coordinated effort by both government and private sector entities to address threats to our Nation’s critical infrastructure.” It will be important for it to take advantage of the public-private relationships already established.

Our April 1998 report also recommended that the President’s Council on Year 2000 Conversion develop a comprehensive picture of the nation’s Year 2000 readiness that would identify and assess risks to the nation’s key

---

economic sectors—including risks posed by international links. In October 1998, the Chair directed the Council's sector working groups to begin assessing their sectors. Accordingly, the Council and federal agencies have partnered with private-sector organizations, such as the North American Electric Reliability Council, to gather information critical to the nation's Year 2000 efforts and to address issues such as contingency planning. To date, the Council has issued three national assessments, most recently on August 5, 1999. These assessment reports have substantially increased the nation's understanding of the Year 2000 readiness of key industries. A similar approach could be used to evaluate longer term risks to our critical infrastructures and provide much-needed pathways for information sharing.

Facilitating Progress and Monitoring Performance

Both the executive branch and the Congress have developed techniques to facilitate and monitor performance in addressing Year 2000 conversion efforts. During 1997, OMB instituted a quarterly reporting routine to facilitate monitoring of agency progress in making their critical systems Year 2000 compliant. Between mid-1997 and early 1999, OMB placed each of the 24 major agencies into one of three tiers according to OMB's judgment regarding each agency's progress as described in their quarterly reports. As yet, no such routine reporting mechanism exists to monitor agency performance in strengthening computer security or critical infrastructure protection. However, as discussed previously, the Critical Infrastructure Assurance Office is reviewing agency infrastructure protection plans. Once these plans are judged acceptable, it will be important to monitor their implementation on a regular basis.

In addition, many congressional committees actively monitored progress by holding hearings to obtain information on the Year 2000 readiness of federal agencies, states, localities, and other important nonfederal entities, such as the securities industry. The House Subcommittee on Government Management, Information and Technology of the Committee on Government Reform developed a “report card” system for periodically grading agencies on their progress.

In addition, to facilitate remediation at federal agencies, the Congress passed and the President signed the Omnibus Consolidated and Emergency Supplemental Appropriations Act, 1999, which included $3.35 billion in contingent emergency funding for Year 2000 conversion activities. In commenting on a draft of this report, the Chairman of the President's Council on Year 2000 Conversion said that the availability of this funding
was of great assistance to agencies during the last 15 months of their conversion efforts and allowed them to fund Year 2000 conversion needs discovered late in the process. The Chairman noted that the situation regarding information security is somewhat different because those efforts will be ongoing rather than tied to a known completion date. Accordingly, agencies should be able to plan to include in their budgets sufficient funding for information security. An alternative view was expressed by the Chairman of the CIO Council Subcommittee on Critical Infrastructure Protection who stated that CIOs would have serious problems implementing PDD 63 without supplemental funding similar to that provided to help resolve the Year 2000 problem.

Developing an Incident Identification and Coordination Capability

To monitor and report on events associated with the Year 2000 date rollover, the President directed establishment of an Information Coordination Center (ICC). The ICC is to serve as the federal government’s central point for coordinating information provided during the Year 2000 transition by government emergency operations centers and the private sector. The center will be staffed with subject matter experts detailed from federal agencies who will be expected to integrate data received into national and international status reports. In this and other ways, the ICC will be expected to highlight information of interest to individual agencies, provide information to the public, and respond to inquiries.

It is currently too early to determine how successful the ICC will be. However, those involved in establishing it are discussing issues that are also pertinent to critical infrastructure protection, such as the amount and type of data the center needs to collect and how this data should be summarized and reported.

Implementing Information Technology Management Improvements

Addressing the Year 2000 problem has highlighted the importance of good information technology management and, to date, demonstrated that the government will likely approach future information technology challenges better prepared. The Year 2000 problem has resulted in many agencies taking charge of their information technology resources in much more active ways than they have in the past, from inventorying and prioritizing systems to implementing reliable processes and better controls. In particular, it has prompted some agencies to establish much-needed information technology policies in areas such as system configuration management, risk management, and software testing. In addition, Year 2000 efforts have reinforced an understanding of the importance of consistent
and persistent top management attention, which is essential to solving any intractable problem. For the Year 2000 problem, this has been illustrated by the work, to date, of the President's Council on Year 2000 Conversion and its senior-level chairman. Such attention from senior federal executives will be important to help ensure that information security and critical infrastructure protection are taken seriously at lower organizational levels and that security specialists have the resources they need to implement an effective program.

According to officials at OMB, the Year 2000 problem also gave agency CIOs a “crash course” in how to accomplish projects. Many CIOs were relatively new in their positions, due to a requirement for agency CIOs in the Clinger-Cohen Act of 1996. Expediting Year 2000 efforts required many of them to quickly gain an understanding of their agency’s systems, work extensively with agency program managers and Chief Financial Officers, and become familiar with budgeting and financial management practices.

Conclusions

The challenges associated with the Year 2000 date conversion problem are examples of the broader and longer term challenges that our nation faces in protecting our computer-supported critical infrastructures from hostile attacks. While differences exist, many of the efforts that have been undertaken to manage and remedy the Year 2000 problem can also be applied to these longer term challenges. Through PDD 63, the executive branch has initiated steps to address critical infrastructure protection and encourage private-sector involvement. As these efforts continue, they can benefit from many of the experiences gained during the Year 2000 conversion period. Some of these “lessons” are already apparent. However, it is likely that others will emerge as the Year 2000 transition period unfolds. Accordingly, we are making no recommendations at this time.

Agency Comments

We provided a draft of this report and solicited informal comments from a variety of officials who have been involved in Year 2000 and critical infrastructure protection efforts. We received oral and electronic mail comments from the Chairman of the Council on Year 2000 Conversion; the Co-Chairs of the CIO Council’s Security Committee, one of whom is Chair of the Subcommittee on Critical Infrastructure Protection; officials in the Critical Information Assurance Office; and numerous federal agency CIOs. Overall, these officials agreed with the points made in the report, and some
provided supporting illustrations from their own experience. We have noted the most significant comments in applicable segments of the report.

As agreed with your office, unless you publicly announce the contents of this report earlier, we will not distribute it until 5 days from the date of this report. At that time, we will send copies to Senator Christopher Dodd, Vice-Chairman of the Senate Special Committee on the Year 2000 Technology Problem; Senator Fred Thompson, Chairman, and Senator Joseph Lieberman, Ranking Minority Member, Senate Committee on Governmental Affairs; Representative Steven Horn, Chairman, Subcommittee on Government Management, Information and Technology, House Committee on Government Reform; and Representative Constance Morella, Chairwoman, Subcommittee on Technology, House Committee on Science. In addition, we are providing copies to John Koskinen, Chairman of the President's Council on Year 2000 Conversion; Richard Clarke, National Coordinator for Security, Infrastructure Protection and Counter-Terrorism; the Honorable Jacob Lew, Director, Office of Management and Budget; John Tritak, Director, Critical Infrastructure Assurance Office; Michael Vatis, Director, National Infrastructure Protection Center, FBI; Deidre Lee and James Flyzik, Chair and Vice-Chair, respectively, of the CIO Council; and other interested parties. Copies will be made available to others upon request.

If you have any questions on matters discussed in this letter, please contact me at (202) 512-2600, or Jack L. Brock, Director, Governmentwide and Defense Information Systems, at (202) 512-6240.

Sincerely yours,

Jeffrey C. Steinhoff
Acting Assistant Comptroller General
Appendix I

Objectives, Scope, and Methodology

The objectives of our work were to (1) summarize our recent findings on computer security and critical infrastructure protection and (2) suggest improvements that build on lessons learned from the Year 2000 date conversion experience.

To summarize our recent findings, we analyzed our reports on computer security issued during fiscal year 1999. In addition, we reviewed findings pertaining to computer security issues associated with the fiscal year 1998 financial statement audits of the 24 federal departments and agencies covered by the CFO Act. These agencies account for 98 percent of the total reported federal net outlays for fiscal year 1998. In analyzing reported findings, we categorized them into six basic areas of general control as described by the Federal Information System Controls Audit Manual (FISCAM), which contains guidance for reviewing information system controls that affect the integrity, confidentiality, and availability of computerized data associated with federal agency operations. These six areas include entitywide security program management and planning, access control, application program change control, segregation of duties, operating systems security, and service continuity. We supplemented this analysis with information that we obtained by reviewing key reports and statements issued since 1994 on critical infrastructure protection. These reports and statements are cited in footnotes throughout this report.

To develop suggested improvements that build on lessons learned from the Year 2000 conversion experience, we analyzed our reports issued since February 1997 on efforts to address the Year 2000 problem and met with key officials leading federal efforts related to the Year 2000 problem and critical infrastructure protection. These officials included the Director of the Critical Infrastructure Assurance Office, the Chairman of the President’s Council on Year 2000 Conversion, officials at the Federal Bureau of Investigation’s National Infrastructure Protection Center, and policy analysts at the Office of Management and Budget involved in overseeing federal Year 2000 conversion efforts and information security.

We provided a draft of this report and solicited informal comments from a variety of officials who have been involved in Year 2000 and critical infrastructure protection efforts. We received oral and electronic mail comments from the Chairman of the Council on Year 2000 Conversion; the Co-Chairs of the CIO Council's Security Committee, one of whom is Chair of the Subcommittee on Critical Infrastructure Protection; and officials in the Critical Information Assurance Office. We considered these comments and noted the most significant ones in pertinent segments of the report.
We performed the majority of our review during August and September 1999 in accordance with generally accepted government auditing standards.
Appendix II

GAO Reports and Testimonies Addressing Information Security Issues Since February 1996

Federal Reserve Banks: Areas for Improvement in Computer Controls

Information Security: NRC’s Computer Intrusion Detection Capabilities

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

Battlefield Automation: Opportunities to Improve the Army’s Information Protection Effort
(GAO/NSIAD-99-166, August 11, 1999).

Information Security: Answers to Post-hearing Questions

Bureau of the Public Debt: Areas for Improvement in Computer Controls
(GAO/AIMD-99-242, August 6, 1999).

Information Security Risk Assessment: Practices of Leading Organizations
(Exposure draft) (GAO/AIMD-99-139, August 1999).

USDA Information Security: Weaknesses at National Finance Center Increase Risk of Fraud, Misuse, and Improper Disclosure

(GAO/T-AIMD-99-223, June 24, 1999).

VA Information Systems: The Austin Automation Center Has Made Progress in Improving Information System Controls
(GAO/AIMD-99-161, June 8, 1999).

Information Security: Many NASA Mission-Critical Systems Face Serious Risks

Department of Energy: Key Factors Underlying Security Problems at DOE Facilities

Information Security: The Melissa Computer Virus Demonstrates Urgent Need for Stronger Protection over Systems and Sensitive Data
(GAO/T-AIMD-99-146, April 15, 1999).
GAO Reports and Testimonies Addressing Information Security Issues Since February 1996


Securities Fraud: The Internet Poses Challenges to Regulators and Investors (GAO/T-GGD-99-34, March 22, 1999).


Federal Reserve Banks: Areas for Improvement in Computer Controls (GAO/AIMD-99-6, October 14, 1998).


Appendix II
GAO Reports and Testimonies Addressing Information Security Issues Since February 1996


Appendix II
GAO Reports and Testimonies Addressing
Information Security Issues Since February 1996

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).


Tax Systems Modernization: Management and Technical Weaknesses Must Be Overcome To Achieve Success (GAO/T-AIMD-96-75, March 26, 1996).

Copies of these products are available through GAO’s home page on the Internet’s World Wide Web (http://www.gao.gov). Copies may also be obtained at GAO’s Document Distribution Center (700 4th St., NW Room 1100) or by phone (202-512-6000) or fax (202-512-6061).


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Year 2000 Computing Crisis: Key Actions Remain to Ensure Delivery of Veterans Benefits and Health Services (GAO/T-AIMD-99-152, April 20, 1999).


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Defense Information Management: Continuing Implementation Challenges Highlight the Need for Improvement (GAO/T-AIMD-99-93, February 25, 1999).


Appendix III
GAO Reports and Testimonies Addressing the
Year 2000 Challenge


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Appendix III
GAO Reports and Testimonies Addressing the
Year 2000 Challenge


Appendix III
GAO Reports and Testimonies Addressing the Year 2000 Challenge


Year 2000 Computing Crisis: National Credit Union Administration’s Efforts to Ensure Credit Union Systems Are Year 2000 Compliant (GAO/T-AIMD-98-20, October 22, 1997).

Social Security Administration: Significant Progress Made in Year 2000 Effort, But Key Risks Remain (GAO/AIMD-98-6, October 22, 1997).


(Based on a list developed by the National Institute of Standards and Technology and included in An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, December 1995.)

- Malicious hackers, those who break into computers without authorization, are especially troubling because their identity and purpose are unknown. In recent years, there has been growing concern that hackers, especially those working on behalf of hostile foreign governments or terrorists, could cause devastating disruptions and damage to computer-dependent operations and infrastructures.

- Malicious code, such as viruses, worms, Trojan horses, and logic bombs, can cause serious damage and disruption and can be costly to remediate. This was recently illustrated by the Melissa virus.

- Errors and omissions in data entry are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all types of users who create and edit data.

- Software programming and development errors can range in severity from benign to catastrophic.

- Installation and maintenance errors can introduce significant security vulnerabilities.

- Criminals intent on fraud and theft can exploit computer systems by automating traditional methods of fraud and by using new methods. Systems that control access to resources, such as inventory systems, are particular targets.

- Employee sabotage can cause especially serious problems because the employee, or ex-employee, may have detailed knowledge of system operations and vulnerabilities. Such sabotage may include destroying hardware or facilities, planting logic bombs that destroy software programs or data, “crashing” systems, or holding encrypted data “hostage.”

- Foreign government espionage efforts, while often thought of as targeting classified systems, may also target unclassified systems to gain information on topics such as travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files.

- Threats to personal privacy are of concern because computers now accumulate vast amounts of electronic information about individuals by governments, credit bureaus, and private companies. In several cases, federal and state employees have sold personal information to private investigators or other “information brokers.”
• Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries.
Appendix V

Examples of Information Security Weaknesses Reported by GAO for Federal Agencies During Fiscal Year 1999

In May 1999, we reported that, as part of our tests of the National Aeronautics and Space Administration’s (NASA) computer-based controls, we successfully penetrated several mission-critical systems. Having obtained access, we could have disrupted NASA’s ongoing command and control operations and stolen, modified, or destroyed system software and data.¹

In December 1998, we reported that weaknesses in Internal Revenue Service’s (IRS) computer security controls continued to place IRS’ automated systems and taxpayer data at serious risk to both internal and external threats that could result in the denial of computer services or in the unauthorized disclosure, modification, or destruction of taxpayer data.²

In August 1999, we reported that serious weaknesses in DOD information security continue to provide both hackers and hundreds of thousands of authorized users the opportunity to modify, steal, inappropriately disclose, and destroy sensitive DOD data. These weaknesses impair DOD’s ability to (1) control physical and electronic access to its systems and data, (2) ensure that software running on its systems is properly authorized, tested, and functioning as intended, (3) limit employees’ ability to perform incompatible functions, and (4) resume operations in the event of a disaster. As a result, numerous Defense functions, including weapons and supercomputer research, logistics, finance, procurement, personnel management, military health, and payroll, have already been adversely affected by system attacks or fraud.³


In July 1999, we reported that the Department of Agriculture's (USDA) National Finance Center (NFC) had serious access control weaknesses that affected its ability to prevent and/or detect unauthorized changes to payroll and other payment data or computer software. NFC develops and operates administrative and financial systems, including payroll/personnel, property management, and accounting systems for both the USDA and more than 60 other federal organizations. During fiscal year 1998, NFC processed more than $19 billion in payroll payments for more than 450,000 federal employees. NFC is also responsible for maintaining records for the world's largest 401(k)-type program, the federal Thrift Savings Program. This program, which is growing at about $1 billion per month, covers about 2.3 million employees and totaled more than $60 billion as of September 30, 1998. The weaknesses we identified increased the risk that users could cause improper payments and that sensitive information could be misused, improperly disclosed, or destroyed.

In October 1998, we reported that general computer controls at the Department of Treasury's Financial Management Service and its contractor data centers placed the data maintained in its financial systems at significant risk of unauthorized modification, disclosure, loss, or impairment. As a result, billions of dollars of payments and collections were at risk of fraud.


Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary, VISA and MasterCard credit cards are accepted, also.

Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC  20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

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

info@www.gao.gov

or visit GAO’s World Wide Web Home Page at:

http://www.gao.gov