United States General Accounting Office

GAO

Testimony

INFORMATION SECURITY

Fundamental Weaknesses Place EPA Data and Operations at Risk

Statement of David L. McClure
Associate Director, Governmentwide and Defense Information Systems
Accounting and Information Management Division

This statement was originally prepared in anticipation of a hearing before the Subcommittee on Oversight and Investigations, House Committee on Commerce, February 17, 2000.

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here to discuss the results of our recent review of information security at the Environmental Protection Agency (EPA), which is being conducted at the request of Chairman Bliley of the House Commerce Committee. In my statement today, I would like to share with you the overall findings and conclusions of our review. We expect to issue a report very shortly to the Chairman which will provide more information about our work and make specific recommendations for corrective actions. In addition, we have informed EPA senior management of our findings to date. Moreover, GAO technical staff have engaged in constructive working sessions with EPA's systems staff in which we have outlined specific problems and discussed options for solutions to immediate vulnerabilities.

Overall, our review found serious and pervasive problems that essentially render EPA's agencywide information security program ineffective. Current security program planning and management is largely a paper exercise that has done little to substantively identify, evaluate, and mitigate risks to the agency's data and systems. Moreover, our tests of computer-based controls have concluded that the computer operating systems and the agencywide computer network that support most of EPA's mission-related and financial operations are riddled with security weaknesses. Of particular concern is that many of the most serious weaknesses we identified—those related to inadequate protection from intrusions via the Internet and poor security planning—had been previously reported to EPA management in 1997 by EPA's Inspector General (IG).

The negative effects of such weaknesses are illustrated by EPA's own records which show several serious computer security incidents in the last 2 years that have resulted in damage and disruption to agency operations. In addition, we identified deficiencies in EPA's incident detection and handling capabilities that draw into question EPA's ability to fully understand or assess the nature of or damage due to its computer security breaches. Accordingly, EPA's computer systems and the operations that rely on these systems are highly vulnerable to tampering, disruption, and misuse. Moreover, EPA cannot ensure the protection of sensitive business and financial data maintained on its larger computer systems or supported by its agencywide network. Our work has sensitized EPA to the seriousness of these issues and agency officials have informed us of some corrective actions and announced other plans which, if properly implemented, can begin to address several of these serious problems.

In my testimony today, I will provide a summary of our findings and conclusions including:

- the specific systems control weaknesses we identified through internal and external penetration testing and how they place EPA's operations and data at risk,
- some examples of recent incidents of computer intrusions and misuse at EPA as well as problems with the practices EPA employs in handling such incidents, and
- the systemic information security management problems that must be addressed in order for EPA to ensure that any corrective actions it takes are effective and remain so on an ongoing basis.

National Concern About Information Security Is Growing

Information security is an important consideration for any organization that depends on information systems and computer networks to carry out its mission or business. Computer security risks are significant, and they are growing. The dramatic expansion in computer interconnectivity and the exponential increase in the use of the Internet are changing the way our government, the nation, and much of the world communicate and conduct business. However, without proper safeguards, these developments pose enormous risks that 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, disrupt operations, or launch attacks against other organization's sites. Further, the number of individuals with computer skills is increasing, and intrusion, or "hacking," techniques are readily available and relatively easy to use. The rash of cyber attacks launched last week against major Internet firms such as Yahoo, eBay, Amazon, E*TRADE, and ZDNet are illustrative of the risks associated with this new electronic age.

Concern about how well federal agencies are addressing these risks is a topic of increasing interest in the both the Congress and the executive branch. This is evidenced by recent hearings on information security, proposed legislation intended to strengthen information security, and the President's recently released *National Plan for Information Systems Protection*.[1] As outlined in this plan, a number of new, centrally managed entities have been established and projects initiated to assist agencies in

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: An Invitation to a Dialog*, issued by the President January 7, 2000.

strengthening their security programs and improving federal intrusion detection capabilities.

Our reports, and those of the agency inspectors general (IG), in the last 5 years describe persistent computer security weaknesses that place federal operations such as national defense, law enforcement, air traffic control, and benefit payments at risk of disruption, fraud, and inappropriate disclosures.[2] This body of audit evidence led us, in 1997 and again in 1999, to designate computer security as a governmentwide high-risk area in reports to the Congress.[3] Our most recent governmentwide summary analysis, which was included in an October 1999 report, noted that significant computer security weaknesses had been identified in 22 of the largest federal agencies.[4] EPA was identified as one of these 22 agencies because EPA's IG had repeatedly reported serious inadequacies in the agency's information security planning, control of Internet services, and monitoring of network activities, as well as an absence of formal firewall technologies to protect EPA from outside intruders.[5] As you know, the work we have conducted for Chairman Bliley that we are discussing today was based largely on his concerns about EPA's progress in addressing these problems.

EPA Is a Major Steward of National Environmental Information

EPA's mission is to protect human health and safeguard the environment. The need to manage its programs for results substantially increases EPA's demand for high-quality environmental information. Such information is also required to identify and respond to emerging problems before significant damage is done to the environment. To fulfill its mission, EPA and the states collect a wealth of environmental data under various statutory and regulatory requirements. In addition, EPA conducts research on environmental issues and collects data through its own environmental monitoring activities.

As the Subcommittee is aware, EPA has spent significant time and resources to develop its information systems and computer networks to

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

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

[4] *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (*GAO/AIMD-00-01*, October 1, 1999).

[5] *EPA's Internet Connectivity Controls,* Office of Inspector General Report of Audit (Redacted Version), September, 5, 1997; *Audit of EPA's Fiscal 1998 Financial Statements*, Office of Inspector General Audit Report Number 99B0003, September 28, 1999.

assist in carrying out its mission. Annually, EPA spends millions of dollars for data collection and information management and technology operations and investments. The integrity and availability of the information maintained on EPA computers is important since it is used to support EPA's analyses, research, and regulatory activities.

Because of the nature of its mission, EPA collects, oversees, and disseminates data and information of varying sensitivity. EPA makes much of its information available to the public through Internet access in order to encourage public awareness and participation in managing human health and environmental risks and to meet statutory requirements. EPA also maintains confidential data from private businesses, data of varying sensitivity on human health and environmental risks, financial and contract data, and personal information on its employees. Consequently, EPA's information security program must accommodate the often competing goals of making much of its environmental information widely accessible while maintaining data integrity, availability, and appropriate confidentiality.

Like many other organizations, EPA's computer environment has changed over the last few years from one involving a centralized mainframe with a highly controlled network to one involving many large computers on a network with nearly unlimited access, including public access through the Internet. This new environment is beneficial because it provides EPA opportunities for streamlining operations and it has provided public access to significant amounts of information. However, as I have just described, this increasingly interconnected computing environment also significantly elevates the risks of inappropriate access to sensitive and critical data. These risks include exposing EPA computers and data to individuals with malicious or criminal intentions, who may want to disrupt or misuse EPA's systems for purposes such as fraud, sabotage, or obtaining sensitive business or personnel data. As a result, EPA, like many other private and government organizations, faces the challenge of balancing the benefits of new technology and Internet use with the new risks such technology introduces. Because such risks cannot be completely eliminated, this balancing act requires a proactive approach to managing information security risks that is dynamic and constantly attentive to changing threats.

EPA's System Access Controls Are Ineffective

Computer systems access controls are key to ensuring that only authorized individuals can gain access to sensitive and critical agency data. They include a variety of tools such as passwords, which are intended to authenticate authorized users; access control software, which

is used to specify individual users' privileges on the system (e.g., read, alter, copy, or delete files); and firewalls, which are to serve as barriers for filtering out unwanted access.

Our tests showed that EPA's access controls are ineffective in adequately reducing the risk of intrusions and misuse. Using widely available software tools, we demonstrated that EPA's network was highly susceptible to intrusions through the Internet and that user and system administrator passwords could be easily accessed, read, or guessed. In addition, we identified weaknesses in all of EPA's computer operating systems that made it possible for intruders, as well as EPA employees or contractors, to bypass or disable computer access controls and undertake any of a wide variety of inappropriate or malicious acts. These acts could include tampering with data; browsing sensitive information; using EPA's computer resources for inappropriate purposes, such as launching attacks on other organizations; and seriously disrupting or disabling computer-supported operations.

Because the weaknesses we identified were associated with the operating systems of EPA's main computers and agencywide network–resources that are referred to as "general support systems"—they affect the security of all of the EPA operations that rely on them. These operations include computer applications that EPA's individual units rely on to carry out their day-to-day operations, such as gathering data on pollutants, research, regulatory enforcement, and financial management.

In short, Mr. Chairman, we identified weaknesses that, if exploited, could have allowed us to control individual EPA computer applications and the data used by these applications. As such, we could have copied, changed, deleted, or destroyed information, thus rendering any security controls implemented for software applications used in specific EPA office networks virtually defenseless.

Although additional details of our review will be in our report, let me briefly describe, at a high level, some of the most significant problems identified by our work.

Ineffective Perimeter Defenses

A firewall and similar perimeter defenses are an organization's first line of defense from outside intrusion. Put simply, a firewall is a software package that controls the content of inbound and outbound computer network traffic, allowing only authorized traffic through its filters. If a firewall is not properly deployed, it may be overly restrictive, thus unnecessarily hindering the flow of network traffic, or it may be too weak, thus providing little or no protection. EPA's firewall and other perimeter

defenses (referred to as screening routers)—designed largely to protect agency systems from unauthorized access from the Internet–were not effective in preventing such intrusions because of weaknesses in the way they were configured and deployed. In our tests, we simulated the type of attacks that might be employed by a computer hacker intruding via the Internet and readily breached and took control of EPA's firewall and other perimeter defenses, thereby gaining access to EPA's agencywide network.

Weak Network and Operating System Controls

Once we successfully penetrated EPA's operating systems, we were able to identify key network components and move throughout the network unimpeded. We were able to take control of EPA's network and could have diverted, altered, or disrupted network traffic. Further, we identified serious vulnerabilities in EPA's major computer systems that allowed us to take control of the systems and the applications supported by them. As a result, by intruding from the Internet, we could have browsed, altered, or deleted data associated with these applications or disrupted their operation.

Poor Password Protections

Our ability to gain access to and take control of EPA's systems was facilitated by the fact that EPA had serious and pervasive vulnerabilities associated with maintaining the confidentiality and integrity of its passwords. These passwords are EPA's primary means of ensuring that access is appropriately restricted to authorized personnel. We obtained passwords in a variety of ways, for example, by guessing them based on our knowledge of commonly used passwords, by viewing and recording them on-line as users keyed them in, and by decrypting encrypted password files with commonly available "password-cracking" software. While on the network, we eavesdropped on computer users' activities, observed them keying in passwords, and used these passwords to obtain "high level" system administration privileges. Such privileges would have allowed us to (1) change system access and other rules, (2) potentially read, alter, delete, or redirect network traffic, and (3) read or tamper with files maintained on EPA's larger computers.

EPA's Systems and Data Have Been Compromised and Misused

EPA's records show that vulnerabilities, such as those I have just described, have been exploited by both external and internal sources. In some cases, these vulnerabilities were exploited because EPA had not corrected known vulnerabilities and properly managed user accounts. Further, they illustrate deficiencies in EPA's ability to detect, respond to, and document security incidents affecting its systems.

The records we analyzed consist primarily of security-related problem reports for 1998 and 1999 that EPA extracted for us from a computerized database, which is maintained at it National Computer Center. EPA has maintained these reports in a computerized database since 1998. By analyzing the database and related records, we identified two dozen instances where security weaknesses were exploited and EPA systems were compromised or misused. EPA's records, while incomplete in many incidents, show that some resulted in damage, disruption, and criminal investigations. In addition, the records showed that EPA was the subject of repeated systematic probes from a variety of domestic and foreign sources. Both the nature and routine pattern of these probes are characteristic of attempts to identify vulnerabilities in EPA's computer network. Such activity often raises concerns that intruders may be preparing for future penetrations. In February 1999, a sophisticated penetration affected three of EPA's computers. EPA was unaware of this penetration until notified by the Federal Bureau of Investigation.

Let me briefly describe some examples that illustrate the types of intrusions and misuse we identified. But, first, let me clarify that these examples were taken from EPA's records; we did not independently investigate them. For many of the examples, we could not determine the full extent of the damage caused by the incidents or how the incidents were resolved because this information had not been documented in EPA's records. For other examples, details cannot be publicly disclosed because the incidents are currently under investigation.

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

- In July 1999, a "chat room" was set up on a network server at one of EPA's regional financial management centers for hackers to post notes and, in effect, conduct on-line electronic conversations. According to EPA, this incident was still under investigation in mid-January of this year.

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

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

- In September 1999, a former subcontractor for an EPA contractor allegedly gained access to an EPA computer and altered the computer's access controls, thereby blocking authorized EPA employees from accessing files. The ability to alter access controls is a privilege that should be restricted to a relatively few trusted individuals. The fact that such alterations were made by a former subcontractor highlights the serious weaknesses in EPA's controls.

Poor Intrusion Detection and Incident Response Capabilities Further Impair EPA's Security

Even strong controls may not block all intrusions and misuse, but organizations can reduce the risks associated with such events if they promptly take steps to detect intrusions and misuse before significant damage can be done. In addition, accounting for and analyzing security problems and incidents are effective ways for an organization to gain a better understanding of threats to its information and of the cost of its security-related problems. In addition, such analyses can pinpoint vulnerabilities that need to be addressed to help ensure that they will not be exploited again. In this regard, problem and incident reports can provide valuable input for risk assessments, help in prioritizing security improvement efforts, and be used to illustrate risks and related trends in reports to senior management.

As part of our reviews of technical controls and of EPA's security problem and incident records, we identified a number of deficiencies in EPA's incident detection and handling capabilities.

- EPA's capabilities for detecting intrusions and misuse are very limited. The automated detection tools EPA has implemented are not effectively deployed, and logs of computer activities are not routinely analyzed to identify unusual or suspicious events or patterns. The effect of these limitations was illustrated by the fact that EPA did not recognize and record much of the activity associated with our test activities. While 23 problem reports were recorded, indicating knowledge about our intrusion testing, none of them recognized the magnitude of our activity and the severity of the security breaches we initiated.

- In most cases, EPA did not assess and document damage or disclosure resulting from individual incidents. Such information is helpful in better understanding security risks and in determining how much to spend on related controls.
- EPA did not routinely analyze problem reports to identify trends and vulnerabilities and apply lessons to other units throughout the agency.
- EPA did not fully follow-up on problems to ensure that they were resolved and that identified vulnerabilities were not repeatedly exploited.
- Problem listings were not protected from browsing. Such protection is important to ensure that intruders or others cannot gain detailed information on security vulnerabilities awaiting correction or monitor the investigations of incidents that they may have originated.
- EPA had not established adequate standards, controls, responsibilities and procedures to ensure uniform and complete management of security problems and responses or clearly differentiated government and contractor responsibilities.
- EPA's central information management office had not routinely summarized and reported security problems and their resolutions to senior EPA management so that they were aware of the magnitude of the problems and related trends.

By addressing these weaknesses, EPA can significantly improve its incident detection and handling capabilities and build on the recordkeeping procedures it has already implemented.

Security Program Planning and Management Is Fundamentally Weak

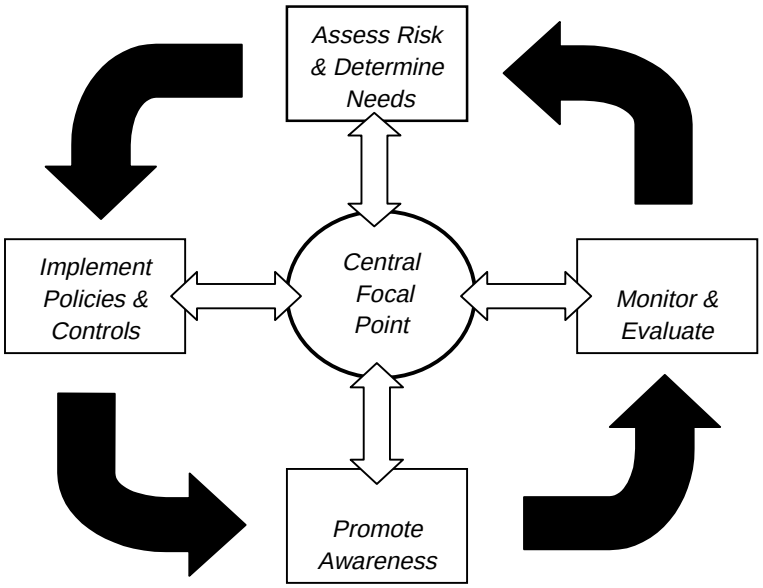
Mr. Chairman, it is imperative that EPA correct the weaknesses that I have described in my testimony today. However, ensuring that computer security controls remain effective on an ongoing basis will require substantial changes to the way EPA approaches its agencywide information security program, especially in regard to (1) assessing risk and determining security needs and (2) ensuring that existing controls are operating effectively. Our review of EPA's security planning and management process found that the Office of Environmental Information, which includes EPA's Chief Information Officer, and EPA's program offices were not adequately working together to ensure that information security risks were fully understood and addressed.

Our own study of leading security management practices used in commercial and nonfederal settings serves to help pinpoint the significant

weaknesses in EPA's computer security program management.[6] We found that these leading organizations manage their information security risks through a cycle of risk management activities. The basic framework—built on 16 specific practices—allows risk management through an ongoing cycle of activities coordinated by a central focal point. This management process, illustrated in figure 1, involves

- assessing risk to determine information security needs;
- developing and implementing policies and controls that meet these needs;
- promoting awareness to ensure that risks and responsibilities are understood; and
- instituting an ongoing program of tests and evaluations to ensure that policies and controls are appropriate and effective.

Figure 1: The Risk Management Cycle



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

This process is generally consistent with OMB and NIST guidance on information security program management, and it has been endorsed by the federal Chief Information Officers (CIO) Council as a useful resource for agency managers. By adopting the risk management principles and practices recommended by our guide, agencies can better protect their systems, detect attacks, and react to security breaches.

Risks Not Fully Considered in Program Office Security Plans

Conversely, EPA's security planning and management practices have been largely a paperwork exercise that have done little to substantively identify, evaluate, and mitigate risks. EPA's policies require each of its major program offices–such as the Office of Water and the Office of Air and Radiation, as well as its Office of the Chief Financial Officer—to determine what levels of protection are appropriate for data and systems supporting their mission-related operations. These offices are also responsible for ensuring that appropriate controls have been effectively implemented before systems become operational. This is appropriate because individual units are the most familiar with the sensitivity and criticality of their data and have the most to lose if poor security negatively affects their operations.

However, our review of individual unit security plans and discussions with responsible officials found that many of EPA's major offices did not fully consider information security risks, clearly define the level of protection needed for their operations, or effectively ensure that controls were implemented effectively. In particular, most units did not adequately consider the security risks associated with the operating systems and agencywide network upon which their individual applications and information systems heavily rely. Nor did they consider other factors affecting the security of their individual systems, such as interfaces with other users' systems. For example, information security plans for some financial applications did not address the risks associated with other financial systems or other program offices' applications that transmit sensitive financial information.

In addition, EPA units did not consistently apply the data risk categories, or sensitivity levels, described in EPA policy as the basis for determining what information security controls were needed. Some units applied other categories or only partially applied EPA's guidance. For example, security plans developed by six of the seven units covered by our review did not identify the overall system sensitivity rating required to determine which set of minimum control requirements outlined in EPA agencywide guidance was appropriate for the systems.

Further, senior officials authorized some systems for processing without testing access controls to ensure that they had been implemented and were operating effectively. Twenty-eight systems had received no management authorization. Such authorizations are important because, according to OMB and EPA guidance, they are intended to represent management's determination that the security of the systems supporting their operations is adequate.

Central Security Management Functions Are Inadequate

While EPA program and business units bear much of the responsibility for ensuring that systems supporting their operations are adequately and effectively protected, EPA's Office of Environmental Information (OEI), which encompasses agency-level information technology management and information security activities, has an essential role to play in providing the needed technical expertise and in effectively implementing technical controls.[7] Our studies of security practices at leading organizations have shown that information security is a responsibility that must be shared by both technical and program staff. This is because, while program offices are in the best position to identify their most sensitive and critical operations and assets, they usually need assistance from technical personnel and security specialists who have current knowledge of the latest threats and of the range of technical controls that can be applied. As in many organizations, most of EPA's technical staff and security specialists who support the agencywide network are organizationally placed under the Assistant Administrator of OEI, who also serves as EPA's Chief Information Officer (CIO).

We found that OEI and its predecessor organization, which was housed under the Office of Administration and Resources Management, had not proactively monitored the effectiveness of information security efforts throughout the agency or provided adequate assistance to program units. While an office within OEI has developed agencywide security policies and conducted some security-related training, neither that office nor any other EPA unit has undertaken the role of facilitating and coordinating implementation of EPA's security policies throughout the agency or ensuring that all systems are periodically tested to ensure that controls are operating effectively.

[7]The Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996 stipulate 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. These acts also require the appointment of a CIO for all federal agencies to help provide the expertise needed to implement effective information resources management.

Our study of leading organizations found that a strong central focal point was important to ensure that policies were consistently understood and implemented and that risks, including those associated with agencywide networks and other broadly used support systems, were fully understood and considered in individual unit plans. In its current formulation, OEI's structural organization and staffing capacity simply do not adequately address the requisite elements of an effective corporatewide security program.

EPA Has an Opportunity to Build on Its Ongoing Information Security Initiatives

The problems I have outlined today pose significant challenges for EPA's entire executive and senior management ranks. The agency established OEI in October 1999 to improve the way it generally manages the large amounts of information it collects and maintains. While this reorganization may result in benefits in other areas of information management, it does not yet appear to have significantly changed the way information security is being managed and addressed throughout the agency.

As I mentioned at the outset, our audit has provided EPA's senior management with specific information on much needed changes. In a meeting with senior OEI management and technical staff in December, we shared some significant security problems uncovered by our testing that, because of their severity, warranted immediate notification and remediation by EPA. This interaction was productive and resulted in quick actions.

Additional changes were outlined 3 weeks ago in a January 28, 2000, memo to EPA executives from the Acting Assistant Administrator for OEI. These included (1) an effort by EPA's Office of Information Collection within OEI to take a broader look at the agency's information protection policies, particularly how the sensitivity of information is determined and (2) establishment of a "Technical Information Security Staff" to rapidly enhance EPA's technical approach to information security. The memo identified the new security staff's key functions as

- developing technical approaches and implementation policies,
- researching and synthesizing best practices,
- supporting senior managers in understanding and carrying out their information security roles,
- educating users and technical staff,

- developing processes and procedures for tracking and reporting security incidents, and

- overseeing the auditing and effectiveness of security programs.

These provisions address many of the management deficiencies we identified, and we encourage EPA to move forward in implementing them. However, effective implementation will require joint efforts by both program and technical staff and a major adjustment in the way EPA considers information security risks and in its management approach. The Technical Information Security Staff will face major challenges in facilitating communication and cooperation among EPA's (1) National Computer Center staff, (2) program, financial, and regional officials, and (3) the various components of the OEI. It will be essential that the new security staff proactively oversee and coordinate security-related activities throughout EPA and ensure that controls are periodically tested, especially those controls that protect the most sensitive and critical of EPA's data.

In summary, Mr. Chairman, EPA is confronted with significant computer security problems that threaten its operations and data. Many of these problems need immediate attention. And like all organizations—public and private—effectively implementing a sustainable information security management program will require top management support and leadership, disciplined processes, consistent oversight, and additional levels of technical and funding support.

This concludes my testimony. I will be happy to answer any questions you or Members of the Subcommittee may have.

(511695)

Ordering Information

Orders by Internet

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

Info@www.gao.gov

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

http://www.gao.gov

To Report Fraud, Waste, and Abuse in Federal Programs

Contact one:

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

E-mail: fraudnet@gao.gov

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