June 2000

INFORMATION SECURITY

Vulnerabilities in DOE's Systems for Unclassified Civilian Research

GAO

Accountability ★ Integrity ★ Reliability

G A O
Accountability * Integrity * Reliability

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

Accounting and Information
Management Division

B-282544

June 9, 2000

The Honorable F. James Sensenbrenner
Chairman
The Honorable Ralph M. Hall
Ranking Minority Member
Committee on Science
House of Representatives

The Department of Energy (DOE) oversees a multibillion-dollar investment in civilian research and development programs at 15 laboratory facilities nationwide. The unclassified information systems that support these programs were designed to facilitate a broad exchange of data and information among scientists around the world. Although unclassified, some of the information in these systems is nevertheless sensitive and requires protection from inappropriate access.[1]

As a result of the growth of the Internet in recent years, these unclassified systems at the DOE laboratories have become increasingly vulnerable to security threats. If exploited, such vulnerabilities could lead to loss or corruption of valuable scientific data, damage to information systems, or disruption of the laboratories' science program operations. According to laboratory officials, such disruptions could cost millions of dollars per day in lost scientific research.

Given the importance of these information systems, you asked us to review the security of information systems that support DOE's unclassified civilian research programs. Our specific objectives were to determine (1) whether DOE's unclassified systems for civilian research are vulnerable to unauthorized access, (2) whether DOE is effectively managing information systems security, and (3) what DOE is doing to address the risk of unauthorized access to unclassified systems for civilian research.

---

[1]The types of sensitive information housed on these systems include Unclassified Controlled Nuclear Information (UCNI), export-controlled information, proprietary information, and information that is designated for official use only.

Results in Brief

Unclassified information systems for scientific research are not consistently protected at all DOE laboratories. Although some laboratories are taking significant measures to strengthen access controls, many systems remain vulnerable. In four recent cases, Internet-based attacks forced specific laboratories to disconnect their networks from the Internet, interrupting scientific research for as long as a week on at least two occasions. Independent reviews conducted recently at various DOE labs confirm significant continuing vulnerabilities. We supplemented these evaluations with our own penetration tests at four DOE laboratories. Our tests showed that two of the laboratories have recently taken steps that would prevent many casual Internet-based attacks. Nevertheless, some DOE systems remain vulnerable.

A major contributing factor to the continuing existence of security vulnerabilities at the DOE laboratories is that DOE has not had an effective program for managing information technology (IT) security consistently throughout the department. We found that DOE lacks key elements of a comprehensive IT security program as outlined in GAO's 1998 Executive Guide.[2] First, no security plans had been prepared for 17 of the 20 major systems in our sample. Furthermore, DOE has not effectively assessed risks. Although all but 2 of the 10 laboratories that we reviewed had performed risk assessments on a laboratorywide level, no system-specific risk assessments had been done for 19 of the 20 systems in our sample. Also, a lack of clear policy on what information is appropriate for public Internet access has led some laboratories to publicly post information on the World Wide Web that could facilitate a potential intruder's attempt to break into DOE systems.

Moreover, line management within the department has not effectively overseen implementation of computer security at the labs. Few on-site audits or reviews have been conducted, and official IT security policies have not been enforced. In addition, DOE has not instituted a consistent and comprehensive program of security incident reporting. While DOE has reported significant improvements beginning in 1999, not all DOE facilities have been reporting incidents to DOE's Computer Incident Advisory Capability (CIAC), and incidents are not consistently reported.

---

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

DOE management is aware that its unclassified security program has been inadequate and recently has taken several steps to improve it, including issuing an updated unclassified IT security policy and developing a five-year action plan. In addition, the department's independent oversight function for information security was strengthened in 1999 and is now more active in reviewing IT security at the laboratories. However, further continuing action will be needed to effectively reform the department's line management oversight structure for IT security.

We are recommending that the Secretary of Energy take immediate steps to strengthen risk-based IT security management at the DOE laboratories, develop a clear and comprehensive line management oversight process, enforce comprehensive and consistent reporting of serious security incidents, establish guidelines for identifying and protecting sensitive electronic information, develop IT security plans for major systems, and institute a mechanism for using laboratory IT security expertise in policy development. In written comments on a draft of this report, DOE said that they were in general agreement with our summary recommendations.

Background

DOE is a large, geographically dispersed organization with diverse activities. Its mission includes furthering scientific understanding of the fundamental nature of energy and matter through research. In fiscal year 2000 the department plans to spend $2.8 billion on many research and development programs at 15 major laboratories nationwide.

Information technology is an essential component for accomplishing DOE's scientific mission. DOE laboratories support their mission with a large and diverse set of computing systems, including very powerful supercomputers capable of performing hundreds of billions of operations per second. The DOE computing environment is highly distributed. Some DOE laboratories have more than 10,000 networked computers. DOE's networks provide over 20,000 scientists across the entire United States and in several foreign countries with access to unique DOE facilities and high-performance computing resources.

Much of the research conducted at the DOE laboratories is unclassified. An open culture exists within the civilian research programs that encourages researchers to freely share scientific discoveries throughout the laboratories and the world research community. Consequently, IT security officials have had to struggle against a widespread belief among scientists that security threats to unclassified systems are less important than

keeping systems and information open and broadly available. DOE has taken steps recently to improve security awareness, such as instituting a mandatory departmentwide security awareness stand down for all employees in August 1999. However, a major challenge facing DOE's security program is to convince senior management officials at the laboratories that effective security measures can be implemented that will not significantly constrain the openness they need for scientific research.

Responsibilities for implementing IT security are spread throughout DOE. The Chief Information Officer (CIO) is responsible for developing IT security policy and guidance throughout the department. DOE laboratories are government owned, contractor operated facilities that operate relatively autonomously. Program managers at each laboratory are responsible for implementing IT security measures in conformance with DOE policy and guidance. DOE's operations offices manage the contracts for the operation of the laboratories. They are responsible for ensuring that the laboratories under their purview are in compliance with DOE security policies and that the implementation of these policies is effective. The lead program secretarial offices at headquarters provide guidance and direction to the operations offices that manage the contracts of the laboratories where their respective programs are concentrated and oversee implementation of information security. The Office of Independent Oversight and Performance Assurance[3] provides independent oversight of IT security activities at the laboratories from DOE headquarters.

Objectives, Scope, and Methodology

Our objectives were to determine (1) whether DOE's unclassified systems for civilian research are vulnerable to unauthorized access, (2) whether DOE is effectively managing information systems security, and (3) what DOE is doing to address the risk of unauthorized access to unclassified systems for civilian research.

To determine whether DOE's unclassified systems for civilian research are vulnerable to unauthorized access, we conducted controlled penetration

---

[3]The Office of Independent Oversight and Performance Assurance is an "independent" oversight organization that has existed in various forms since 1982. This office, originally called the Office of Security Evaluations (OSE), was organized under DOE's Office of the Assistant Secretary for Defense Programs. In 1990, OSE was moved to DOE's Office of the Assistant Secretary for Environment, Safety, and Health. OSE became the Office of Independent Oversight and Performance Assurance in 1999 and now reports directly to the Secretary of Energy.

tests of systems at four DOE laboratories that host several civilian research systems. At DOE's request, we arranged with the Computer Incident Advisory Capability (CIAC) to test and evaluate the department's technical controls for ensuring that data and systems at the laboratories are protected from unauthorized access by sources external to the laboratories. We independently performed an additional test at one of these laboratories to assess the lab's protection from unauthorized access by internal sources. We established the scope of the tests performed by CIAC and our technical team and monitored both teams' progress. We informed DOE in advance of all tests to be conducted and obtained their concurrence. We limited the tests to unclassified civilian research systems agreed upon in advance with officials from the laboratories. At the conclusion of the tests, the Computer Protection Program Manager (CPPM) at each laboratory was provided the test results, including recommendations for correcting the specific weaknesses identified. In addition, we reviewed findings from an independent assessment performed by the private sector firm Internet Security Systems (ISS) on another DOE laboratory's unclassified systems. We also reviewed reports and assessments on computer security prepared by DOE's independent oversight office and CIAC. From statistics in CIAC reports, we analyzed the number and types of computer security incidents at the DOE laboratories for the last 3 years.

To evaluate whether DOE is effectively managing unclassified information systems security, we requested and obtained specific information from the CPPMs at 10 of DOE's 15 national laboratories. In order to focus on major facilities for unclassified civilian research, we selected laboratories receiving substantial funding from DOE's Office of Science. We reviewed laboratorywide IT security plans, policies, and procedures, as well as IT security reviews and audit reports for each of the 10 laboratories. We also requested additional information on 20 major computing facilities, systems, and networks supporting research programs at these laboratories. This information included IT security and contingency plans, risk assessments, system authorizations, and security reviews and audit reports. We did not attempt to verify the accuracy or completeness of the information provided by the laboratory CPPMs.

Based on this information, we compared DOE's practices with the Office of Management and Budget (OMB) Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, which was last updated in February 1996. In addition, we compared DOE's practices with guidelines in two National Institute of Standards and Technology (NIST) publications,

Generally Accepted Principles and Practices for Securing Information Technology Systems (Spec. Pub. 800-14, September 1996) and *An Introduction to Computer Security: The NIST Handbook* (Spec. Pub. 800-12, October 1995). Based on our analysis of the documentation provided and discussions with department officials, we determined whether DOE's practices were in compliance with federal IT policies as well as DOE's own guidance. We also used our May 1998 executive guide, *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68). Our guide identifies key elements of an effective information security program, describes practices that eight leading nonfederal organizations have adopted, and details the management techniques these leading organizations use to build information security controls and awareness into their operations. This guide has been endorsed by the federal government's CIO Council, which is cochaired by OMB's Deputy Director for Management and a federal agency CIO.

To review what DOE is doing to address the risk of unauthorized access to unclassified systems for civilian research, we reviewed official policy, procedure, and guidance documentation. In addition, we held discussions with key department officials responsible for the IT security program, including the CIO, security officials within the Office of the CIO and the Office of Science, and members of the System of Laboratories Computer Coordinating Committee (SLCCC). We conducted site visits at six of the national laboratories funded by the Office of Science where we were briefed by officials responsible for IT security. We also interviewed officials from DOE's Office of Independent Oversight and Performance Assurance.

We performed our audit work from April 1999 through March 2000 in accordance with generally accepted government auditing standards.

Many DOE Systems Are Vulnerable to Attack

The threat of attacks to DOE systems has grown dramatically in recent years. Several successful attacks have had a significant impact on civilian research program operations at specific laboratories. Although our tests showed that the laboratories have recently taken steps to protect themselves against unsophisticated Internet-based attacks, we nevertheless found vulnerabilities at all of the laboratories that a knowledgeable intruder could exploit.

Computer Security Incidents at DOE Laboratories Have Increased Dramatically

The DOE laboratories have become a popular target of the hacking community. Although few of the laboratories consistently report all computer security incidents at their sites, the number, variety, and seriousness of those that have been detected and reported have grown dramatically in recent years. As shown in figure 1, there was a 17-fold increase in the number of incidents reported between 1997 and 1999 alone.

Figure 1: Reported DOE Laboratory Computer Security Incidents
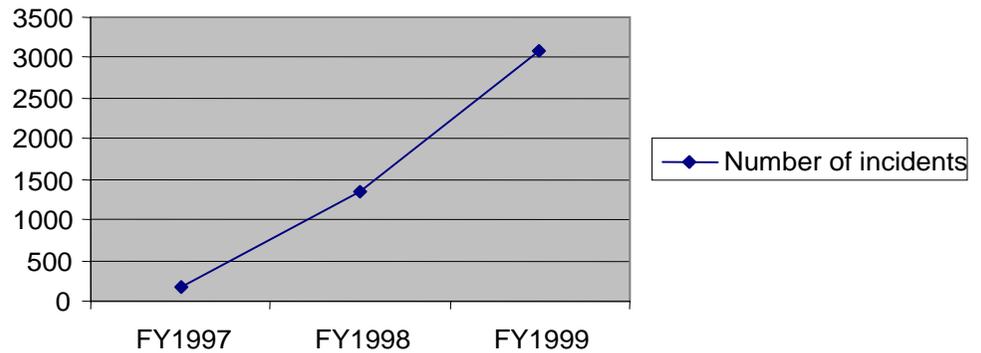
These reported incidents include intrusions, attempted intrusions, inundation of servers with junk e-mail, insertion of malicious codes into computers, scans and other probes, and denial-of-service attacks.[4] In fiscal year 1999, scanning and probing activities made up 75.4 percent of reported incidents. Because these activities are often precursors to an attack, they point to the hacker community's substantial interest in DOE laboratories.

The threat has intensified in part because of the dramatic increase in the number of individuals, sites, and regions of the world that can connect to DOE laboratories through the Internet. Another contributing factor is that known vulnerabilities and automated attack tools for exploiting them are increasingly being publicly posted on the Internet, enabling attackers with little technical skill and knowledge to potentially cause much damage.

---

[4]A denial-of-service attack renders a computer system unusable by consuming, damaging, or destroying some or all of its internal computing resources.

While some reported incidents may represent mere nuisances, others can be serious. In the last 2 years alone, 253 successful attacks were reported at all DOE sites. Of these, we identified 4 cases where the targeted laboratories were forced to temporarily disconnect their networks from the Internet, disrupting the laboratories' ability to do scientific research for up to a full week on at least two occasions:

- In June 1998, a hacker successfully launched an attack on a DOE laboratory from a compromised machine at another DOE site using the Unix remote login command. Once on the remote system, he exploited that machine's "trust relationship"[5] with other systems to quickly compromise 40 to 50 user accounts on more than 30 machines. Normal operations at the laboratory were significantly affected by this attack. Resolution of the problem required cutting off Internet access and changing all passwords to accounts on the compromised machines, a process that took a week to complete.
- In July 1998, files were modified at another DOE laboratory when a hacker exploited a known software vulnerability to break into an electronic mail server. The laboratory was forced to shut down access to the Internet while all passwords were changed, thereby adversely affecting all research activities at the laboratory during that period.
- In August 1999, users and system administrators were caught unprepared when a hacker launched an automated denial-of-service attack that compromised over 20 systems at one DOE laboratory within 3 minutes. The heavy traffic that resulted from the attack soon flooded the laboratory's network, preventing communication among the lab's computers. In the course of the attack, malicious software code was successfully planted on 27 computer systems. The laboratory was forced to disconnect their networks from the Internet to terminate and recover from the attack.
- In October 1999, system administrators at another DOE laboratory discovered that a hacker had entered their systems through an improperly configured computer. To resolve the security breach, the laboratory had to disconnect all its networks from the Internet for 1 week while passwords for all user accounts were changed.

---

[5]A "trust relationship" allows users on one system to freely access other systems in the relationship, as if those other systems were simply extensions of the user's own system. Thus, a hacker who gains access to one system in such a relationship can then access all the other systems that trust it.

Our tests showed that some DOE laboratories have recently taken steps to strengthen access controls on many of their systems. For example, several of the laboratories we tested had effectively reduced their vulnerability to Internet-based attack by limiting the number of potential software connections to their machines. Several of the laboratories also required strong user authentication and provided users with secure communications capabilities. Nevertheless, we identified significant residual vulnerabilities at some of these sites.

Poor Access Controls Jeopardize DOE Systems

A broad range of technical controls can be used to help ensure that only authorized users gain access to an organization's information resources. Such controls include

- perimeter defenses, including firewalls, which keep unauthorized external traffic from entering local networks, and intrusion detection systems, which try to spot unauthorized activity as soon as it happens;
- controls on access to individual computers, such as passwords, which may be used to authenticate users; and
- mechanisms to protect specific files of information, such as "permissions," which limit user privileges to read, alter, copy, and delete specific data.

During our penetration testing at four DOE laboratories, our team tested the access controls of major systems supporting unclassified civilian research. We also reviewed recent independent reports on computer security vulnerabilities at DOE laboratories to identify additional findings related to access controls. From these activities, we identified a range of security vulnerabilities that a knowledgeable intruder could exploit.

Poor Perimeter Defenses

Perimeter defenses provide organizations with a first line of defense against outside intruders. Firewalls (or other perimeter defenses such as filtering routers) keep unauthorized traffic from entering local networks. Intrusion detection systems employ a variety of methods to examine network activity for indications of potential unauthorized use. We found that several DOE laboratories had not effectively implemented such defenses to protect their internal systems from intrusions from the Internet, thus jeopardizing their computer systems and networks.

We found that one laboratory was directly connected to two external networks, with no restrictions on what kinds of traffic could enter through these connections. Furthermore, the same laboratory was excessively

permissive in allowing inbound Internet traffic through its main Internet gateway. The laboratory placed restrictions on only two of the Internet's many services. We identified potential vulnerabilities in some of the unrestricted services that, if exploited by intruders, could be used to gain access to more than 200 of the laboratory's systems.

Two of the laboratories that we tested relied heavily on intrusion detection systems as a key element of their security strategy to protect their computer networks. Officials at one of these laboratories stated that their intrusion detection's strong monitoring and detection capabilities allowed them to avoid imposing stricter access controls on their systems. However, as demonstrated by our tests, these systems have significant limitations. Although our activities were eventually caught by the intrusion detection systems, we were nevertheless able to obtain detailed technical information about most of the systems at these sites, including potentially vulnerable and important machines. It is possible that a potential intruder, working stealthily over an extended period of time, could gain access to these machines without being detected.

Moreover, intrusion detection systems provide no protection against intruders who are able to pose as legitimate users through the use of compromised passwords. Since as much as 60 percent of the serious incidents at the DOE laboratories involve compromised passwords, the heavy reliance of these two laboratories on intrusion detection is risky.

Poor User Authentication

In the past, most computer systems have used simple, unencrypted (cleartext) password systems to control user access. However, in a highly networked environment such as DOE's, cleartext passwords provide only modest protection since they can be "sniffed" (i.e., intercepted) by any compromised system in the network path. Because this is a fairly common method used by hackers to gain unauthorized access, security officials from the laboratories have set a goal to replace cleartext passwords with more sophisticated means of authenticating users. Nevertheless, many DOE laboratory systems encountered in independent reviews and our tests continued to rely on cleartext passwords to control user access.

For password-controlled systems, recent independent reviews have repeatedly found that DOE laboratory system administrators failed to perform basic security practices in password protection. Such failures include not configuring their systems to store password information in encrypted form, allowing users to choose passwords that are relatively

easy to guess, and, in some cases, not requiring the use of passwords at all, which would allow a hacker to copy, alter, or delete any file on that system.

Our tests confirmed that even simple password-based protection was not being properly managed in some cases. We also found some machines with user accounts that were not password protected at all. In addition, we found user accounts with weak passwords on systems that had trust relationships with many other systems. A hacker who broke the password for one of these systems, which we were easily able to do, could then immediately access all the other machines that trust it. Using a widely available password-cracking tool found on the Internet, we succeeded in breaking passwords from several systems.

Poor File Protection

Individual files of data that are resident on systems require their own access controls, apart from network and system-level controls. Much of the information stored on DOE civilian research systems, although unclassified, is sensitive and must be protected from unauthorized access. Furthermore, inadequately protected files can often help intruders significantly extend their unauthorized access and activities.

Reports issued by DOE's Office of Independent Oversight and Performance Assurance in 1998 noted that public Internet users could freely access many DOE sensitive documents, including Unclassified Controlled Nuclear Information, Official Use Only, Export-Controlled Information, and Cooperative Research and Development Agreement Information. In 1999, an independent contractor's network analysis and penetration test further discovered that unauthorized users were being allowed multiple access paths to internal systems.

On several occasions, independent assessments have also found that technical information, such as system password files and network diagrams, that would greatly assist potential intruders could be easily obtained. Furthermore, our test team was successful in obtaining detailed technical information about most of the targeted systems, information that would significantly assist a potential intruder in trying to break into those sites. For example, several sites allowed users to execute a command that would provide a complete inventory of the site's host computers, their Internet Protocol (IP) addresses, and the types of devices. For a potential intruder, this feature would greatly simplify the task of identifying potential targets for attack. We also found systems that openly provided lists of valid user names, which could assist intruders in guessing passwords, thus giving them a head start in gaining unauthorized access.

A review performed by the Office of Independent Oversight and Performance Assurance also documented a lack of proper controls on users' ability to upload new files or alter existing files on DOE networks. One assessment found that 35 percent of one laboratory's anonymous File Transfer Protocol (FTP) servers were insecurely configured. Another report noted that unauthorized users could modify system files. Hackers, taking advantage of these weak access controls, can store illegal software on DOE laboratory computers and alter the content of DOE Web pages. Our testing showed that file protection vulnerabilities persist. For example, one of the tested laboratories had not disabled several commands known to give intruders the ability to remotely change password files, create new files, or even delete any file on the system. Web servers with known vulnerabilities remained unfixed, allowing intruders to replace laboratory home pages with unauthorized content. We also found that many sensitive system files, such as those establishing trust relationships, were not protected. This weakness could also allow hackers to masquerade as any authorized user they chose to be, including the system's administrator.

Management of DOE's Unclassified Security Program Has Been Ineffective

A major contributing factor to the existence of the security vulnerabilities discussed above is that DOE did not have an effective program for managing IT security consistently throughout the department. During our review, we found that DOE lacked several of the key elements of a comprehensive IT security program as outlined in our 1998 Executive Guide. DOE did not prepare required IT security plans. Nor did the department effectively identify and assess information security risks. In addition, DOE has not provided adequate policy guidance on what information is appropriate for public Internet access. Moreover, line management oversight of computer security implementation at the laboratories was inadequate. And finally, reporting of security incidents was neither consistent nor comprehensive.

DOE System Managers Are Not Preparing Required IT Security Plans

GAO's 1998 *Executive Guide* notes that successful organizations view information protection as an integral part of strategic planning. Furthermore, federal guidance requires IT security plans to be prepared as part of agencies' information resources management planning process. OMB Circular A-130 requires agencies to develop system security plans for each major application. DOE policy also directs computer security officials to formulate, continually update, and annually review computer protection plans for each laboratory, as well as for multiple computer installations, computer systems, or program-area applications.

However, we found that DOE installations were not developing the required IT security plans. Although plans had been prepared for each laboratory, system-level plans had not been prepared for 17 of the 20 systems in our sample. Without system security plans, laboratory officials have no basis for determining how consistently or effectively security controls have been implemented. For example, during our testing, we found that security controls had been implemented inconsistently across the various platforms within two laboratory divisions and that these controls were not integrated with laboratorywide controls. As a result, we could have penetrated the system.

Furthermore, many of the laboratorywide security plans provided by DOE were incomplete. Half of the plans did not address controls over interconnections with other systems, a fundamental requirement for security planning listed in OMB Circular A-130. Given the extensive networking of DOE applications and laboratories to each other and to the Internet, as well as the potential impacts should these networks be compromised or unavailable, the lack of planning for the risks and controls over system interconnections is especially dangerous.

DOE Does Not Effectively Assess Risks

Risk assessment is a crucial first step in managing a consistent and effective IT security program. Although all but two of the laboratories had performed risk assessments on a laboratorywide level, no system-specific risk assessments had been done for 19 of the 20 major IT systems in our sample. Furthermore, more than half of the laboratorywide risk assessments that we did obtain lacked key elements required by DOE policy, including the identification of the value of the IT assets, potential threats, and system vulnerabilities.

Federal guidance requires all agencies to develop comprehensive IT security programs based on assessing and managing information security risks. According to GAO's November 1999 Executive Guide,[6] identifying and assessing information security risks in terms of the impact on operations is an essential step in determining what controls are needed and what level of resources should be expended on controls. In this regard, understanding the risks associated with information security is the starting point of the IT security management cycle. DOE policy regarding

[6]*Information Security Risk Assessment: Practices of Leading Organizations* (GAO/AIMD-00-33, November 1999).

unclassified IT security requires that periodic risk assessments be conducted for computer systems prior to their becoming operational, upon significant change, or at least every 2 years. Security reviews conducted by DOE at two of the laboratories in our sample have previously identified a lack of documented risk assessments. Nevertheless, at the time of our review, DOE was still not effectively using risk assessments to manage its IT security program.

OMB Circular A-130, Appendix III, also requires management officials to formally authorize use of a system prior to its becoming operational, upon significant change, and at least every 3 years thereafter. DOE managers, however, are not properly authorizing their systems for use. Not one of the 20 systems in our sample provided documentation of system authorization.

Our testing of the security at one laboratory demonstrated that risk assessments conducted on a laboratorywide level do not provide managers with adequate information to measure risks to their individual systems. Although a laboratorywide assessment had been conducted and threats to the laboratory's overall network infrastructure identified and the risks accepted, managers with whom we spoke were unaware of the vulnerabilities of their particular systems. Consequently, they had taken little action to address these vulnerabilities. In relying solely on the laboratorywide assessment, they erroneously assumed that their systems had been provided adequate security.

Moreover, a comprehensive implementation of the risk assessment process could help to resolve the tensions that exist between DOE researchers, who are primarily concerned with open and collaborative scientific research, and department IT security officials, who struggle to ensure the integrity and availability of unclassified IT systems and the information they contain. Because risk assessments not only identify and document risks but also clearly establish program managers' accountability for mitigating them, the risk assessment process would force program managers to carefully and systematically analyze the threats and vulnerabilities of their systems and consciously assess the need to apply adequate countermeasures.

DOE Lacks Guidance on the Protection of Sensitive Information From Public Internet Access

DOE has not developed guidelines specifying the extent to which sensitive information should be protected from public Internet access. The DOE laboratories host many public World Wide Web sites. One of the laboratories that we visited, for example, was operating 163 separate sites, representing each of the laboratory's divisions as well as individual projects undertaken by those divisions. The volume and nature of the resources at these sites can provide a wealth of information for researchers and hackers alike. Although DOE policy requires that the laboratories provide all information with protection that is commensurate with its sensitivity, appropriate safeguards have not been consistently implemented when information is posted to the Web.

During our audit we found sensitive information publicly available through DOE Web sites that could facilitate electronic intrusions. For example, in August 1999 we found 10 detailed maps of one laboratory's local area networks posted on a Web site, including a map of the lab's entire internal network. This information could be used to facilitate an intruder's attempt to break into the lab's systems. These network maps had been publicly available since March 1996.

The laboratories have identified problems in this area and recognize the need for specific guidelines for establishing the sensitivity of information and systems. For example, one OSE audit report that we reviewed noted:

[A] troublesome area in [the lab's] unclassified computer security program is that users and administrators cannot always identify, and thereby properly protect, mission-essential or sensitive unclassified information. Interviews with [the lab's] computer users and systems administrators showed that not all individuals have the necessary training or guidance . . . to adequately determine information sensitivity. Actual dissemination of such guidance to appropriate personnel varies widely. . . . Further, the guidance given is inconsistent with the critical and sensitive information list for operations security. As a result, several staff responsible for determining information sensitivity had not done so. In some of those instances, Privacy Act and Proprietary CRADA [Cooperative Research and Development Agreement] information was not being properly controlled and protected. Because [the lab's] users and administrators cannot always identify the data they process as being sensitive, appropriate safeguards cannot be implemented to protect it . . . consequently, the data remain at risk of compromise.

The audit team also emphasized their concerns regarding the need to identify and adequately protect sensitive information:

[T]he number and severity of . . . problems, centering on identification and protection of sensitive information, raise fundamental concerns about the site's ability to meet protection requirements. The ongoing vulnerabilities to network penetration, as well as the associated

risks presently being assumed, have serious implications given the amount, sensitivity, and technological and monetary value of information.

DOE Management Does Not Effectively Oversee Implementation of Computer Security at the Laboratories

DOE management has not effectively overseen implementation of unclassified IT security at its laboratories. The oversight roles and responsibilities of organizations at headquarters and in the field require a layered approach to IT security oversight. However, few management oversight reviews have been conducted at any level and official policies have not been enforced. Moreover, DOE management has not followed up on the results of internal reviews and thus cannot ensure that identified security problems have been corrected.

Few Management Reviews Have Been Conducted

As discussed in GAO's 1998 *Executive Guide*, oversight is a key element of managing IT security. By conducting periodic reviews, line management can monitor compliance with policies, assess the continuing effectiveness of security countermeasures, and correct newly identified vulnerabilities. Independent oversight reviews complement line management reviews by providing an objective outside view. OMB Circular A-130 mandates that security controls of critical IT systems be independently reviewed or audited at least every 3 years. Furthermore, DOE policy calls for management and compliance reviews to be conducted routinely. We reviewed both independent oversight reviews and line management reviews conducted at DOE's civilian research laboratories.

Few independent oversight reviews of unclassified IT security management have been conducted at the DOE laboratories in recent years. We requested that the 10 laboratories in our survey provide copies of all security reviews and audits performed over the last 3 years for each of the laboratories as a whole as well as for the 20 major systems in our sample. The laboratories provided us with documentation showing that several internal audits and security reviews had recently been conducted by the laboratories themselves. They also provided copies of vulnerability assessments sponsored by the laboratories and conducted by DOE's Computer Incident Advisory Capability (CIAC).[7] However, only three laboratories provided evidence of independent reviews, all of which were conducted by DOE's

---

[7]CIAC, DOE's incident reporting and response organization, conducts vulnerability assessments when requested by the laboratories. However, the results of these reviews are reported only internally to the requesting laboratory and not to any DOE headquarters organizations.

independent oversight organization. At the system level, no evidence of external management reviews was provided for any of the 20 systems in our sample.

DOE's field operations offices, which are the line organizations directly responsible for ensuring that the laboratories comply with DOE's IT security policies,[8] have not been conducting IT security compliance reviews. Each operations office has a Computer Protection Program Coordinator (CPPC) who is responsible for overseeing implementation of security at the laboratories under their purview.[9] We met with the CPPCs at two of the three operations offices responsible for the laboratories funded by the Office of Science. They informed us that they have not performed any audits or security reviews of unclassified IT security. The CPPC at one office told us that their oversight activities were strictly limited to reviewing performance measures adopted in response to identified security vulnerabilities at the labs. Officials at another office referred us to a 1995 memo from headquarters placing a moratorium on audits and oversight reviews of the laboratories by both DOE headquarters and the field operations offices until a performance-based evaluation program could be piloted. They stated that because they had never been informed of new processes or procedures to evaluate performance, no line management reviews of unclassified computer security had been undertaken.

The headquarters Office of Science, which is responsible for monitoring the Oakland, Oak Ridge, and Chicago field operations offices, has not conducted any reviews to assess how well the operations offices have been overseeing unclassified IT security at the laboratories since 1993. In the past, DOE headquarters officials reviewed the operations offices' processes for evaluating laboratory performance every 2 years, but this practice ended 7 years ago. According to Office of Science officials, their oversight activities since 1993 have been limited to analyzing the results of

---

[8]DOE policy mandates that the operations offices conduct compliance reviews every 2 to 3 years to assess the adequacy of protection plans and the continuing effectiveness of security procedures at the laboratories.

[9]The Chicago Operations Office has responsibility over Ames Laboratory, Argonne National Laboratory, Brookhaven National Laboratory, Environmental Measurements Laboratory, Fermi National Accelerator Laboratory, New Brunswick Laboratory, and Princeton Plasma Physics Laboratory. The Oakland Operations Office has responsibility over Lawrence Berkeley National Laboratory, Lawrence Livermore National Laboratory, and Stanford Linear Accelerator Center. The Oak Ridge Operations Office is responsible for Oak Ridge National Laboratory and Thomas Jefferson National Accelerator Facility.

annual surveys conducted by the operations offices to determine the effectiveness of their implementation of policies. These surveys have relied heavily on the labs' self-assessments. Furthermore, until a departmental reorganization in 1999, unclassified IT security was excluded from these surveys.

Deficiencies From Reviews Have Not Been Resolved

Although the laboratories themselves have conducted several internal audits and security reviews, DOE management has not consistently followed up on the security deficiencies that have been identified by these and other reviews. As a result, security weaknesses have often gone unresolved. For example, of the eight laboratories in our sample that provided multiple audit reports, six continued to operate with deficiencies that were repeatedly identified in subsequent audits. And, of the 17 audits that reported the same recurring deficiencies in subsequent reports, more than half presented no evidence that any follow-up activities had been undertaken to address the previously reported findings. These findings involved problems such as a failure to implement the required self-assessment program and inadequate protection of sensitive data.

Moreover, DOE has no process for tracking the laboratories' implementation of CIAC-recommended actions. Because the results of the laboratories' security evaluations are kept in strict confidence, DOE management cannot monitor whether the laboratories have taken corrective action to fix vulnerabilities identified by these assessments.

DOE Laboratories Do Not Fully and Consistently Report Incidents

As stated in GAO's 1998 *Executive Guide*, summary records of actual security incidents can provide valuable input for risk assessments and budgetary decisions. Recognizing this, OMB Circular A-130 requires agencies to establish formal mechanisms dedicated to evaluating and responding to security incidents in a manner that protects the agency's own information and helps to protect the information of others who might be affected by the incident. These formal incident response mechanisms should also share information concerning common vulnerabilities and threats with those in other systems and other agencies. DOE policy also mandates incident reporting.

DOE's CIAC was established in 1989 to help and protect the DOE community. In addition to providing the laboratories with round-the-clock assistance in responding to security incidents, CIAC also identifies and publicizes security vulnerabilities in commercial software as they are discovered, recommending actions to fix these flaws.

However, CIAC's effectiveness has been limited. Although 3,072 incidents were reported in fiscal year 1999, these statistics do not reflect the overall vulnerability of the agency because only a few DOE sites were reporting to CIAC. At the time of our review, approximately 75 percent of DOE sites had not reported incidents to CIAC in the previous 3 years. In commenting on a draft of this report, the Office of the CIO provided updated information indicating that most of the science laboratories are now reporting incidents to CIAC. However, the reports that CIAC receives are not always consistent. While some sites report all incidents, others report only those they consider critical. Still others contact CIAC only when they need assistance in responding to an incident. Moreover, according to laboratory officials, DOE laboratories are increasingly reluctant to use CIAC resources, because a recent 17-fold increase in the number of incidents reported to them has impeded CIAC's ability to respond promptly to the laboratories' requests for assistance.

The lack of consistent and comprehensive incident reporting hinders DOE's ability to assess the effectiveness of its management of IT security. Furthermore, laboratory reluctance to use CIAC resources for incident response undermines the department's ability to identify and disseminate critical information about emerging threats, information that would allow other laboratories to bolster their own security posture.

DOE Is Taking Steps to Improve But Challenges Remain

The DOE CIO has recently initiated several significant actions to strengthen the management of the department's unclassified security program. In July 1999 the CIO issued an updated unclassified computer security policy that requires each DOE organization to develop a plan that documents its unique security program.[10] The policy clearly states that the plan must account for the organization's specific environment, missions, and threats and detail the approach to ensuring effective cyber security. It must address roles and responsibilities, access controls, and risk assessment processes and document a host of other specific aspects of security. Furthermore, the policy institutes a three-level review process for each organization based on a self-assessment every 2 years, a peer review every 3 years, and independent oversight. The Office of Independent Oversight and Performance Assurance has begun a program of increased oversight inspections, reviews, and testing and plans to cover six science

---

[10]DOE N 205.1 Unclassified Security Program. N 205.1 requires all DOE organizations to submit their plans by January 2000.

laboratories in 2000. The laboratories will be required to draft and implement corrective action plans to address shortfalls uncovered by the reviews. The CIO plans to issue additional IT security guidance by the end of the fiscal year and also has developed a program action plan that lays out and schedules a set of activities to fully implement the new policy over the next 5 years.

These are positive steps that are aimed at addressing the department's greatest weaknesses in unclassified IT security. However, implementing the new policy consistently throughout the department will not be possible without establishing new processes and practices such as standardized risk management procedures. Also, developing mechanisms such as audits, reviews, and processes for tracking and measuring follow-up actions will be essential for overseeing and enforcing the new policy. Furthermore, establishing a much tighter management framework than currently exists will be necessary to effectively coordinate the diverse roles and responsibilities of each of the offices in the management chain between the laboratories in the field and the Office of Science at DOE headquarters.

Finally, it is essential to continuously update departmental policies and develop supplemental guidelines to address technical issues and gaps as they become apparent. Advisory groups that possess a high level of technical expertise along with an understanding of the DOE research community environment could assist the Office of the CIO in these efforts. A good example is the existing System of Laboratories Computer Coordinating Committee (SLCCC) Technical Working Group, whose members are drawn from the DOE laboratory environment and which has previously assisted the CIO's office in establishing divisionwide policy.

Conclusions

Serious vulnerabilities in IT systems at the DOE national laboratories could have an impact on the department's ability to perform its scientific research. A major contributing factor to the existence of these vulnerabilities is that DOE has not had an effective program for managing IT security consistently throughout the department. DOE recognizes the need to bolster its program and has recently taken steps to improve. However, effective change will require implementing a stronger framework of management accountability and additional specific policy guidance. Until these are achieved, DOE cannot ensure that its unclassified civilian research systems are adequately protected at all DOE national laboratories.

Recommendations

We recommend that the Secretary of Energy take immediate steps to strengthen the management of the department's unclassified computer security program. Specifically, we recommend that the following actions be taken:

- Establish guidelines for a consistent risk-based approach to IT security management. Require all of DOE's scientific laboratories to identify all their critical systems and formally assess the potential threats and vulnerabilities of each system before operation, upon significant change, or at least every 3 years. Require that managers document that this process has been followed, what level of protection they have determined is appropriate, what controls they have selected to provide this protection, and that they accept responsibility for any residual risks.
- Develop a clear and comprehensive line management oversight process to continuously monitor and enforce the laboratories' compliance with departmentwide policy and the effectiveness of established controls. The process should include audits and reviews and establish clear roles and responsibilities for each organization in the line management chain and procedures for tracking identified vulnerabilities and for ensuring that follow-up actions are implemented.
- Establish mechanisms to enforce reporting of all serious security incidents to CIAC. We further recommend that the Office of the CIO establish and issue guidelines to clarify what types of incidents must be reported. At a minimum, these types must include all incidents that could adversely affect scientific research through compromises of mission data or computational resources.
- Establish guidelines for determining the sensitivity of electronic information and the extent to which such information should be publicly accessible through the Internet and establish management oversight processes to ensure compliance with this guidance.
- Ensure that headquarters-based reviews identify and correct shortcomings in draft annual security plans prepared by the science laboratories. Specifically, the plans should identify which systems are critical for the laboratories to achieve their scientific missions and how these systems are interconnected, both within the lab and externally. The plans should also outline the procedures used by the laboratories to assess threats and vulnerabilities and regularly test whether the countermeasures employed to protect these systems are effective in mitigating identified risks.
- Develop a mechanism for effectively integrating the skills and expertise of staff at the DOE laboratories in the development of official policy and

guidance. The CIO should consider chartering the existing SLCCC Technical Working Group in this capacity.

We also recommend that the DOE CIO review the specific vulnerabilities and suggested actions provided to laboratory CPPMs at the conclusion of our testing; determine and implement appropriate security countermeasures; and track the implementation and disposition of these actions.

Agency Comments and Our Evaluation

In written comments on a draft of this report, which are reprinted in appendix I, DOE's Director, Office of Security and Emergency Operations, stated that the department was in general agreement with our summary recommendations. In an attachment to the letter, DOE provided information on actions it is taking that relate to our recommendations as well as additional comments on the substance of our findings. Based on their comments, we clarified three of our recommendations and provided additional clarification in the body of the report.

In its letter, DOE raised two concerns about our draft: that (1) many of the issues and problems we raised came from internal DOE reports dated 1998 and earlier and that (2) our staff seemed to confuse existing DOE policy with previous departmental policy. We disagree with the department about both of these issues. First, our discussion of vulnerabilities at the DOE science laboratories is based primarily on tests that we conducted in 2000 or that were conducted for us by CIAC in late 1999. These results were supplemented by test results that were independently obtained within the last 2 years. While it is true that some of the results discussed in our report date to 1998, they are not the primary sources for our discussion of vulnerabilities. Two minor references in the draft report's discussion of vulnerabilities were based solely on test results dated earlier than 1998. These two references have been deleted from the final report.

Regarding the second concern, DOE provided two specific citations[11] that led the department to conclude that our staff were confused about DOE policy. The first of these citations in our report clearly refers to OMB guidance rather than DOE policy. Our concern is with fulfillment of the requirement under OMB Circular A-130 that security plans address controls over interconnections with other systems. Our report makes no reference to any specific DOE policy, past or present, that may interpret OMB A-130 guidance. The second citation in our draft report refers to how we characterized DOE's policy on IT security risk assessments. Our draft stated that they should be conducted every 5 years, whereas current DOE policy requires risk assessments every 2 years. That detail has been corrected in the final version and does not affect any of our findings, conclusions, or recommendations.

As agreed with your office, unless you publicly announce its contents earlier, we plan no further distribution of this report until 5 days from the date of this letter. At that time, we will send copies of this report to the Honorable Bill Richardson, Secretary of Energy, and the Honorable Jacob J. Lew, Director, Office of Management and Budget. Copies will be available to others upon request. If you have any questions, please call me at (202) 512-6240. Major contributors to this report include Gary Austin, Lon Chin, John de Ferrari, Elizabeth Johnston, Harold Lewis, Duc Ngo, Tracy Pierson, Jamelyn Smith, and Christopher Warweg.

Jack L. Brock, Jr.
Director, Governmentwide
and Defense Information Systems

---

[11]The citations appear on pages 10 and 11 of the department's letter.

Comments From the Department of Energy

Department of Energy
Washington, DC 20585

23 May 2000

U.S. General Accounting Office
ATTN: Mr. Jeffrey C. Steinhoff
Acting Assistant Comptroller General
Accounting and Information Management Division
441 G. Street, NW
Washington, D.C. 20548

Dear Mr. Steinhoff:

The Department of Energy (DOE) appreciates the opportunity to review and comment on
the General Accounting Office (GAO) draft report entitled "Information Security:
Vulnerabilities in DOE's Systems for Unclassified Civilian Research" (GAO/AIMD-00-
140), dated June 29, 2000.

Cyber security is a challenge for both Government and industry where, at the present and
in the foreseeable future, there are no "silver bullet" fixes or perfect solutions. Rather, as
GAO has noted, an effective security program is achieved through a balance of policy,
procedures, technology, and training. Any system connected to the Internet (either
directly or indirectly) is vulnerable to an attack. Since the spring of 1999, the Secretary
of Energy and the Chief Information Officer have emphasized a Departmentwide focus
on cyber security in the wake of vulnerabilities discovered at our Defense facilities. This
initial focus subsequently was extended to all DOE sites, including the Science
Laboratories. While we are not satisfied with protection of our information assets at all
of our sites, we recognize that there has been tremendous improvement during the past
year and assuming adequate fiscal support from Congress, additional improvements are
planned for the next 18 months.

We are concerned about two issues in the GAO report. First, many of the issues and
problems raised by the GAO team came from 11 internal DOE reports, most of which
were dated 1998 and earlier. While these reports reflect the state of cyber security years
ago, they do not accurately reflect the current state of cyber security within the
Department as the sites involved have been continuously working to improve in this area.
The intermixing of dated findings with results discovered in the year-long GAO audit
may cause readers to draw incorrect conclusions regarding the Department's present state
of cyber security. Furthermore, technology upgrades are frequent in the Department,
occurring about once every two years in the Science Laboratories. Therefore, most
computers and networks that supported DOE sites in 1998 and earlier have been
upgraded or replaced. Second, the audit staff seemed to confuse existing DOE policy
with previous Departmental policy. For example, the report references DOE Order
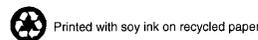
Printed with soy ink on recycled paper

1360.2B, Unclassified Computer Security Program (May 18, 1992), which was replaced by DOE Notice 205.1, Unclassified Cyber Security Program, dated July 26, 1999. We have spoken to your staff regarding these issues and recommend appropriate revisions be made to the draft report.

GAO tested cyber security access controls at four DOE Science National Laboratories— Stanford Linear Accelerator Center (SLAC), Lawrence Berkeley, Lawrence Livermore, and Argonne, —and found 84 significant security weaknesses. GAO found 1 weakness at SLAC, 2 weaknesses at Lawrence Livermore, 3 weaknesses at Lawrence Berkeley and 78 weaknesses at Argonne. The site and DOE management have been aggressively addressing each. Of the 84 weaknesses, 55 were corrected immediately (i.e., within days of notification). These corrections include all weaknesses at SLAC, Berkeley and Livermore National Laboratories, and 49 of the identified weaknesses at Argonne. Of the remaining 29 weaknesses identified at Argonne, all will be corrected by July 2000. The Department's Office of Independent Oversight and Performance Assurance had previously scheduled a review of Argonne's cyber security program for November 2000. However, due to the weaknesses uncovered at Argonne in GAO's review, we have requested that this review be moved to August 2000 to permit the Department to review the effectiveness of the program at Argonne and fixes to the weaknesses identified by GAO. The results of the Independent Oversight review at Argonne will be shared with GAO and Congress.

Enclosed is the DOE response to issues raised in the report. If you have any questions regarding the Department's comments or would like to discuss them further, please contact me on (202) 586-3345, or John M. Gilligan, Chief Information Officer, on (202) 586-0166.

Sincerely,
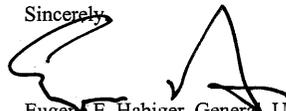
Eugene E. Habiger, General, USAF (Retired)
Director, Office of Security and
  Emergency Operations

Enclosure

2

**DEPARTMENT OF ENERGY COMMENTS ON GAO DRAFT REPORT
ENTITLED "INFORMATION SECURITY: VULNERABILITIES IN DOE'S
SYSTEMS FOR UNCLASSIFIED CIVILIAN RESEARCH"**

Department Comments on Recommendations

During the past year, and concurrent with the conduct of GAO's review of DOE's
unclassified civilian research facilities, the Department of Energy completely restructured
its cyber security program. In May 1999, the Department created a Cyber Security Office
under the Department's Chief Information Officer. Four new cyber security policies and
two guidelines were developed and issued during the past year, completely revising
previous guidance on unclassified cyber security. Each site has developed a detailed
cyber security plan to describe the implementation of these new policies and guidelines.
The Department has also completed a rapid training program to improve the security
skills of our less experienced Systems Administrators, with over 2,000 System
Administrators trained as of May 15, 2000. A separate training course was provided to
line managers.

At the direction of Secretary Richardson last summer, the Department conducted daylong
security awareness "stand downs" at all sites to ensure that all DOE employees were
aware of security threats, Departmental policies, and personal responsibilities. A cyber
security metrics program has been initiated to measure progress at each DOE site and to
focus management attention on problem areas. A DOE Cyber Security Architecture
Guideline that will help ensure consistency of protection at our sites has been drafted. In
addition, in May 1999, a proactive independent security assessment organization was
established, the Office of Independent Oversight and Performance Evaluation, reporting
directly to the Secretary. For the past year, this Independent Oversight office has been
conducting thorough reviews of cyber security effectiveness at DOE sites. Finally, the
Department has doubled the size of its central cyber security incident response capability
at Lawrence Livermore National Laboratory, the Computer Incident Advisory Capability
(CIAC).

In short, the cyber security program in the Department in May 2000 bears little
resemblance to the program in place a year ago. While the Department is not yet
satisfied with the level of protection that we have achieved to date, we believe that the
initiatives that we have taken over the past year have dramatically improved security
within the Department. Furthermore, we believe that the Department is on track to
demonstrating an effective security program implementation at all sites in the near future.

In reviewing the report, in addition to not reflecting recent efforts in cyber security, some
information used by GAO is extremely dated. In some cases, conclusions noted in the
report are based on information from DOE oversight reviews that are over two-years old,
and therefore, do not reflect the current security posture at DOE sites or even the systems
and networks that are presently in place (due to rapid technological evolution). The
Department believes that there are a number of instances where the draft report misleads

3

the reader regarding the current state of cyber security in the Department. In addition, in some cases, references to DOE cyber security policies appear to reflect obsolete policies. Specific instances of these problems are included in the Section of the response entitled "Department Comments on Findings" below.

Despite concerns from the Department regarding potentially misleading references in the report, DOE is in general agreement with the summary recommendations made by GAO. Implementation of each of GAO's recommendations has either been completed or is well underway. Actions to address each of the recommendations are summarized below. Based on the actions discussed below, the Department believes that it is approaching an effective cyber security program for our unclassified civilian research facilities.

See comment 1.

Recommendation #1: Establish guidelines for a consistent risk-based approach to IT security management.

The Department issued DOE Notice 205.1, Unclassified Cyber Security Program, on July 26, 1999, which establishes the policy for the Department's unclassified cyber security program and sets forth requirements and responsibilities. The Notice requires each DOE organization to prepare a Cyber Security Program Plan (CSPP) and update it at least every two years.

DOE Notice 205.1 requires each organization to address 13 different elements in the organization's CSPP. The elements include the following:

- cyber security roles and responsibilities
- cyber boundary protection
- configuration management policies
- incident response and reporting
- CSPP change management (i.e., impacts of technology, threat environment, or other changes)
- cyber security controls (technical and non-technical)
- operational threat, risk, and vulnerability assessment processes
- cyber security training methodology
- methodology to address malicious code
- CSPP compliance assessment processes
- CSPP peer review selection process
- organizational mission interoperability clusters (groups of systems/capabilities requiring uniform protection)
- organization management by name and title

These CSPP elements closely align with the five risk management principles outlined in GAO's May 1998 Executive Guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-68).

To date, all 12 Science Laboratories within the Department have developed CSPPs. Ten of the Laboratory CSPPs have completed review by Headquarters DOE organizations and

4

See comment 2.

have been found to meet or exceed compliance requirements. The remaining two CSPPs are still undergoing Headquarters DOE review and will be completed no later than June 22, 2000.

To further emphasize risk-based management, the Department is developing a cyber security architecture. The architecture will require each organization to manage risk by assessing impacts to business operations and implementing effective controls consistent with the cyber security architecture guidelines and commensurate with the assessed level of risk. Completion of the DOE cyber security architecture is anticipated in July 2000.

Recommendation #2: Develop a clear and comprehensive management oversight process to continuously monitor and enforce the laboratories' compliance with Departmentwide policy and the effectiveness of established controls.

The Department has developed and documented a multilevel management oversight process for cyber security. In May 1999, the Secretary of Energy established a direct reporting relationship with the Office of Independent Oversight and Performance Assurance (Independent Oversight) to provide feedback on the effectiveness of line management implementation of Departmental security policy. As part of this effort, the newly established Office of Independent Oversight created and staffed a cyber security office. The Office of Independent Oversight maintains a robust vulnerability and penetration testing capability and conducts a full schedule of comprehensive assessments that include both performance testing and programmatic evaluations.

Since May 1999, the Office of Independent Oversight has conducted 17 reviews of cyber security programs. For the remainder of calendar year 2000, the Office of Independent Oversight plans to conduct an additional 15 reviews. The reviews consist of a combination of external network security assessments, on-site inspections, and penetration tests. The Office of Independent Oversight plans to conduct reviews at each DOE site every 18 months.

In addition to the Office of Independent Oversight reviews, the Department's Office of Inspector General and Office of Counterintelligence also conduct cyber security reviews for specific missions and line organizations. Since August 1999, the Office of Counterintelligence has completed six cyber security reviews and expects to complete five additional reviews by December 2000. The Department is also beginning a continuous three-year peer review process cycle, in accordance with DOE Notice 205.1.

Responsibilities of the Office of the Chief Information Officer and DOE line management organizations were also defined by Secretary Richardson in May 1999 and are summarized in DOE Notice 205.1. The CIO is responsible for cyber security policy development and overall oversight of the Department's cyber security program. Line management organizations, including Headquarters Secretarial Offices and Intermediate Offices (Operations and Field) are responsible for monitoring organization implementation of policy, ensuring adequate resources are applied to cyber security, and accepting residual risks through the coordination and approval of CSPPs.

5

See comment 3.

Recommendation #3: Require all DOE Laboratories to consistently report serious security incidents.

DOE N 205.1 requires Laboratories to report serious cyber security incidents. Each DOE organization is required to provide 24-hour-a-day, 7-day-a-week coverage for incident reporting. DOE policy also requires that DOE organizations specify in their site security plans (i.e., CSPP) the type of events that require monitoring, the "enclaves" and systems subject to monitoring, how the 24x7 monitoring is handled, and the composition of the organization incident response team. DOE organizations must also provide security incident information to the National Infrastructure Protection Center and the DOE Office of Counterintelligence, as necessary.

As of May 15, 2000, 11 of 12 Science Laboratories have approved procedures for reporting cyber incidents. In fiscal year 1999, 10 of 12 Science Laboratories reported cyber incidents to CIAC. Since the beginning of fiscal year 2000, 9 of 12 Science Laboratories have reported such incidents to the Computer Incident Advisory Capability (CIAC) at Lawrence Livermore National Laboratory in California. CIAC reporting statistics have been provided to GAO.

See comment 4.

Recommendation #4: Establish guidelines for determining the sensitivity of electronic information and the extent to which such information should be publicly accessible through the Internet.

The Department reissued "Guidance for Providing Information to the Public via Public Access Servers" in June 1998. The document describes steps for determining if information is appropriate for public consumption and how it should be posted to public access servers to ensure data integrity and availability. Public access servers include electronic bulletin boards, file transfer protocol servers, gopher servers, and the World Wide Web. The URL for the Guide is http://cio.doe.gov/ucsp/pdfphil/PAS1.PDF. Although this Guide is easily accessible from the CIO home page, it probably is not widely disseminated or consistently followed throughout the Department. Moreover, the Guide is several years old and will be updated this summer.

The Department has also issued DOE Order 241.1. & DOE Guide 241.1, "Scientific and Technical Information Management" which require DOE programs to ensure that Scientific and Technical Information (STI) including scientific and technical software, is reviewed for sensitivity (including non-proliferation and national export control).

The Department realizes that screening information to determine that it is appropriate for Internet publication is a challenging task. The Department will continue to seek other Federal Agencies with a suitable "model" policy in this area.

See comment 5.

Recommendation #5: Institute a headquarters-based review process to ensure that the laboratories prepare annual security plans as required by departmental policy.

6

This recommendation is accomplished through DOE Notice 205.1, effective July 26, 1999, which requires Departmental Elements to prepare an organizational Cyber Security Program Plan (CSPP) within 180 days after issuance of the Notice. In addition, DOE Notice 205.1 requires CSPPs to be updated at least every two years. The basic elements of the CSPP are listed in the response to Recommendation #1 above. The Notice also established a Headquarters-based review process. As of May 16, 2000, 89 sites have submitted CSPPs, of which 83 have been reviewed.

DOE Notice 205.1 also established a three-level review process for CSPPs, including a Headquarters-based review. In addition to reviews of the CSPPs prior to formal approval, the Office of Independent Oversight plans to assess the effectiveness of the implementation of CSPPs through on-site inspections. Results of the reviews are briefed to the Secretary, Deputy Secretary, and senior line management. Corrective action plans are developed to address weaknesses identified in the reviews. Progress on implementing the corrective action plans are monitored by the DOE Security Council, chaired by the Director of the Office of Security and Emergency Operations (i.e., DOE Security Czar) who reports directly to the Secretary. In addition, each organization completes a self-assessment of its approved CSPP implementation at least every two-years. Finally, building on the strength of the academics culture of DOE Laboratories, peer reviews are required to be conducted at least once every three-years.

See comment 6.

Recommendation #6: Develop a mechanism for effectively integrating the skills and expertise of staff at the DOE laboratories in the process of developing official policy and guidance.

Since the spring of 1999, all DOE cyber security policies have been developed through extensive coordination and consultation with the Laboratories. DOE Notice 205.1, dated July 26,1999, formalized this coordination and consultation process by chartering the (cyber security) Policy Working Group (PWG) and the Technical Working Group (TWG). These groups include representation from DOE Laboratories and Program Offices and have been specifically formed to assist in the formulation of policy and guidance, as well as to provide technical advice to the CIO. The groups were formed in January 2000. To date, the PWG has met twice, and the TWG has met once. The Department believes that the two groups are providing an effective collaborative means to develop official policy and guidance leveraging the extensive expertise in our Laboratories.

Recommendation #7: Review the results of GAO's penetration testing at specific Science Laboratories.

GAO tested cyber security access controls at four DOE Science National Laboratories—Stanford Linear Accelerator Center (SLAC), Lawrence Berkeley, Lawrence Livermore, and Argonne, —and found 84 significant security weaknesses. GAO found 1 weakness at SLAC, 2 weaknesses at Lawrence Livermore, 3 weaknesses at Lawrence Berkeley and 78 weaknesses at Argonne. Of the 84 weaknesses, 55 were corrected immediately (i.e., within days of notification). These corrections include all weaknesses at SLAC, Berkeley

7

and Livermore National Laboratories, and 49 of the identified weaknesses at Argonne. Of the remaining 29 weaknesses identified at Argonne, DOE and site personnel are aggressively working to resolve the vulnerabilities, and all will be corrected by July 2000. The Department's Office of Independent Oversight and Performance Assurance had previously scheduled a review of Argonne's cyber security program for November 2000. However, due to the number of significant security weaknesses uncovered at Argonne in GAO's review, we have requested that this review be moved to August 2000 to permit the Department to review the effectiveness of the security program at Argonne and fixes to the weaknesses identified by GAO. The results of the Independent Oversight review at Argonne will be shared with GAO and Congress.

General Comments

See comment 1.

The GAO report references the Office of Management and Budget (OMB) Circular A-130, Appendix III, Security of Federal Automated Information Resources, which was updated in February 1996. This Circular requires Federal organizations to conduct system-specific risk assessments and develop system-specific security plans. DOE has found that even well-protected individual systems are vulnerable to weaknesses in interconnected systems. DOE Notice 205.1, Unclassified Cyber Security Program, dated July 26, 1999, emphasizes protection of interrelated "systems of systems" (enclaves and clusters of computing systems) as well as entire organizational sites. Changes in technology over the past four-years since Appendix III was last updated have significantly changed the nature of a "system" and "application" from a security protection standpoint. In this regard, we recommend that this focus be added to OMB A-130 in the next update.

We acknowledge that our policy, which focuses on security plans for sites and "systems-of-systems," does not have an emphasis on security plans for individual applications (as correctly noted by GAO). DOE Notice 205.1 requires that each organization determine if individual applications should have separate security plans (i.e., CSPPs). The Department does, however, emphasize risk management for individual components (networks, hosts, and applications) in DOE Notice 205.1 and will reemphasize the requirement for system risk assessment in the DOE cyber security architecture document that will be published in July 2000.

See comment 2.

In addition, we believe the GAO audit team use of the term "oversight" may confuse readers of the report. In some cases, GAO uses oversight to refer to performance evaluation and monitoring functions performed by line management and, in other cases, to refer to the independent oversight performed outside of line management channels. Within DOE, line management provides guidance on implementation of policy and subsequent monitoring of compliance with Departmental guidance. The DOE independent oversight function, on the other hand, serves as a feedback mechanism to the Secretary and senior management on the effectiveness of implementation of the Department's policies for unclassified cyber security. We request that the report be modified to make a clear distinction between performance evaluation functions

8

conducted by line management and the internal oversight function performed by the DOE Office of Independent Oversight and Performance Assurance.

Department Comments on Findings

The following section addresses the issues the Department believes do not accurately depict the current state of cyber security within the Department of Energy. The comments below are directed primarily to the text found under the draft GAO report section entitled "Results in Brief" but include corrections to other portions of the report as well.

Page 3, Paragraph 2: We disagree with the statement that "the Department has not provided adequate management oversight of computer security at the labs."

See comment 2.

Comment: It is noted that there is no timeframe included in this reference in the report. Since the spring of 1999, the Department has implemented a number of initiatives to ensure proactive oversight of cyber security at DOE Laboratories and facilities. In May 1999, the Secretary of Energy clearly assigned policy responsibility for cyber security to the Office of the Chief Information Officer and charged line management with oversight of cyber security implementation. The Secretary also established the Office of Independent Oversight and Performance Assurance to report on the effectiveness of implementation of Departmental security policy. This Office has a full schedule of comprehensive assessments (that include both performance testing and a programmatic review), remote vulnerability testing, and follow-up reviews to assess line-management implementation of cyber security across the DOE complex.

Since the Secretary's reorganization in May 1999, there has been a much greater visibility on Office of Independent Oversight cyber security assessments as well as a high priority on implementing prompt corrective actions. Senior management (including the Secretary, Deputy Secretary, Assistant Secretary, Field Managers, and Site Managers) are briefed on the results of each Independent Oversight assessment. Line managers are responsible for rapid development of corrective action plans to resolve identified issues. Follow-up action plans are monitored through the DOE Security Council, which is chaired by General Eugene E. Habiger, Director of Security and Emergency Operations. This process has been ongoing for about one year. DOE Order 470.2A, Security and Emergency Management Independent Oversight and Performance Assurance Program, dated March 1, 2000, establishes the requirements and responsibilities for responding to Office of Independent Oversight assessments.

In addition to the roles and responsibilities specifically associated with Independent Oversight, DOE Notice 205.1 establishes a three-tier review process, which includes organization self-assessments, peer reviews, and oversight reviews. These reviews are done on a periodic basis from annually to triennially.

9

Page 3, Paragraph 2: The statement that "about 25 percent of all DOE facilities have been reporting incidents to DOE's Computer Incident Advisory Capability (CIAC)" is incorrect.

See comment 3.

Comment: As discussed in Recommendation #3, DOE Notice 205.1 states "DOE organizations must report security incidents to the organization incident response team and to CIAC. In addition, each DOE organization must provide 24-hour-a-day, 7-day-a-week coverage." As of May 15, 2000, 11 of 12 Science Laboratories have approved procedures for reporting cyber incidents. In fiscal year 1999, 10 of 12 Science laboratories reported cyber incidents to CIAC. Since the beginning of fiscal year 2000, 9 of 12 Science laboratories have reported incidents to CIAC. DOE is actively working with the Federal CIO Council and FedCIRC to help establish a Governmentwide standard or agreement on what should be reported to a central incident reporting organization, such as CIAC and FedCIRC.

Now on p. 3.

Page 3, Paragraph 3: This is a misleading statement and an unfair characterization.

See comment 7.

Comment: DOE management is aware that its unclassified security program has been inadequate and recently has taken several steps to improve.

Page 5, Paragraph 2: We strongly disagree with the statement that "This unguarded attitude has prevailed despite many reported attacks carried out against these systems".

See comment 8.

Comment: The Department and its Laboratories have greatly increased the awareness among senior management that cyber security is critical. Lessons learned from successful attacks that some sites experienced in the past has been shared across the complex. In addition, the extensive visibility given to this area by Secretary Richardson over the past year has increased the awareness and attention by top management. Visible evidence of this increased attention included a mandatory Departmentwide security awareness "stand down" for all employees in August 1999, in order to emphasize Departmentwide security awareness and to conduct employee training.

Now on p. 13.
See comment 9.

Page 20, Paragraph 3: We are unclear on the GAO reference in this paragraph. The reference may apply to plans prepared in the past under DOE Order 1360.2B, Unclassified Computer Security Program, dated May 18, 1992, rather than security plans prepared under the current policy in DOE Notice 205.1, dated July 26, 1999. The current policy requires that Departmental Elements prepare CSPPs that address interconnectivity controls. At a minimum, we request that GAO reword the paragraph to reflect the current policy.

Now on p. 14.

Page 21, Paragraph 2: DOE disagrees with the statement that "DOE's policy regarding unclassified IT security requires that periodic risk assessments be conducted for computer systems prior to their becoming operational, upon significant change, or at least every 5 years."

10

See comment 10.

Comment: Again we believe that GAO has confused what policies are in effect. DOE Order 1360.2B, Unclassified Computer Security Program, dated May 18, 1992, which included the 5-year criteria, is no longer in effect. Its replacement, DOE Notice 205.1, which has been in effect since July 26, 1999, requires that each Departmental Element assess threats, risks, and vulnerabilities of information systems identified in its CSPPs at least every two years.

Now on p. 20.

Page 31, Paragraph 1: DOE disagrees with the statement that "The CIO has also developed a program action plan that lays out and schedules a set of activities to implement the new policy over the next five years."

See comment 11.

Comment: Although it is true that DOE's cyber security action plan addresses activities the Department plans to carry out over the next five years, the Department's cyber security policies are implemented when issued.

11

The following are GAO's comments on the Department of Energy's letter dated May 23, 2000.

GAO Comments

1. The department's comments do not address major elements of our recommendation, including (1) the requirement that the science laboratories identify all critical systems and formally assess the potential threat and vulnerabilities of each system, and (2) the requirement that managers document that this process has been followed, what level of protection they have determined appropriate, what controls they have selected to provide this protection, and that they accept responsibility for any residual risks. In its "General Comments," DOE discusses these elements at more length, acknowledging that DOE policy does not have an emphasis on security plans for individual applications. DOE also acknowledges that OMB guidance requires federal organizations to conduct system-specific risk assessments but says it will recommend that OMB A-130 be changed in the future.

   We disagree with DOE's suggestion that individual risk assessments are not appropriate for highly interconnected systems for three reasons: (1) A key element of the risk-based approach to information security is that the managers of systems understand the risks they face and take responsibility for the security of their systems. They do this by conducting risk assessments and formally authorizing their systems for operational use. If this process is conducted only at the level of an entire national laboratory, individual system managers will not be involved and cannot effectively be held accountable for the security of their systems. (2) Extensive interconnections are indeed pervasive in the Internet age. However, this fact should be a factor in the risk assessment process rather than a basis for deferring system-level risk assessments. Even at the "enclave" or laboratory level, DOE systems are highly connected through the Internet to many other sites, such as universities and foreign research facilities, that DOE cannot control from a security standpoint but must consider as elements of risk. Individual systems within those laboratories are no different. System managers need to consider the risks of their interconnections, both internally as well as to the outside world, when they conduct risk assessments. (3) Individual systems, though interconnected, are still subject to system-based threats and vulnerabilities. Controls on access to individual computers, such as passwords that may be used to authenticate users, are part of the range of technical controls used to

help ensure that only authorized users gain access to an organization's information resources. In this regard, it remains critical that risk assessments be performed for individual systems.

2. DOE's comments focus largely on the oversight activities associated with the Office of Independent Oversight and Performance Assurance, which have been enhanced over the past year. We are aware of these improvements and acknowledge them in the report. Our continuing concern, however, is that a process be established whereby line management actively monitors performance and enforces compliance with DOE policy. DOE's comments mention the responsibilities of line management organizations as promulgated in key policies but provide no indication that a process has been established to ensure that these actions take place or that they are effective in enforcing compliance with departmentwide policy.

   We have edited the discussion of management oversight and the associated recommendation to clarify our concern with line management's responsibility for enforcing compliance with DOE policy.

3. We agree with DOE that official department policy requires the reporting of serious cyber security incidents. At the same time as their comments were submitted, DOE provided updated statistics from CIAC on reported incidents that show an increase in the number of science laboratories reporting incidents to CIAC. According to the new information, most laboratories are now reporting incidents. The final report has been updated to reflect this recent information. However, we have not received any updated information to indicate that DOE has clarified the types of incidents that must be reported or that the laboratories are now consistently reporting all "serious" incidents. We have modified our recommendation to stress the need for DOE to clarify the types of incidents that must be reported and for DOE line management to enforce compliance with this policy.

4. We agree with the department that screening information to determine that it is appropriate for Internet publication is a challenging task. Based on our audit findings, we believe the department can and should take greater steps in this area. For example, the guidance referred to by the department is focused on considerations for public posting of various types of information, including sensitive information. It does not address the problem of determining the sensitivity (and associated security risks) of the information itself. Furthermore, the department

admits that this guidance is probably not widely disseminated or consistently followed throughout the department.

We have clarified our recommendation to focus on determining the sensitivity of electronic information and establishing management review processes to ensure that such information is properly protected from inappropriate electronic access.

5. We agree with DOE that a basic headquarters-based review process has been established and we consider that a valuable step forward. However, our recommendation chiefly addresses the concern that the new review process correct deficiencies that we identified during our audit. For example, since many of the laboratory plans we reviewed did not discuss interconnections with other systems, we recommended that the laboratories' plans identify these interconnections as well as outline procedures for assessing threats and vulnerabilities and testing countermeasures. We have not yet received any information to show that the laboratories have addressed these issues in their new plans. Our recommendation has been clarified to focus on the need to ensure that the content of the annual plans addresses weaknesses we identified during our review.

6. We are aware that DOE in 1999 chartered the two working groups mentioned in the department's comments. However, during the course of our review, these groups, though chartered, had not met. DOE does not cite specifically how these groups are working to revise policies. In contrast, the SLCCC, referenced in our report, has been very active and has provided unofficial input to the CIO on key IT security topics. Thus, it remains unclear from DOE's comments how extensively the department wishes to capitalize on IT expertise at its science laboratories. Accordingly, we believe that the simple existence of the PWG and TWG is not adequate to address our recommendation.

7. Both the draft and final versions of our report reflect the exact wording of the department's comment.

8. We are aware that the department has taken steps in the last year to increase awareness of IT security issues throughout the national laboratories. However, we remain concerned that the institutional culture at the science laboratories resists the imposition of many types of security controls. We have modified the text to acknowledge that the

department has taken steps in the last year to improve awareness of IT security issues.

9. As stated in both the draft and final versions of our report, our concern is with fulfillment of the requirement under OMB Circular A-130 that security plans address controls over interconnections with other systems. The paragraph makes no reference to any specific DOE policy, past or present, that may interpret OMB guidance.

10. We have corrected the final version of the report to address the department's concern.

11. In its comment, DOE acknowledges that our draft report statement is correct. The department also states that cyber security policies are implemented when issued. As demonstrated by our findings related to line management oversight and reporting of security incidents, it is not always true that policies are implemented when they are issued.

Ordering Information

The first copy of each GAO report is free. Additional copies of reports are $2 each. A check or money order should be made out to the Superintendent of Documents. 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

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

Orders by phone:
(202) 512-6000
fax: (202) 512-6061
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.

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, or 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)

PRINTED ON RECYCLED PAPER

United States
General Accounting Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Correction Requested