United States General Accounting Office

GAO

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

May 1998

COMPUTER SECURITY

Pervasive, Serious Weaknesses Jeopardize State Department Operations

GAO

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

Accounting and Information
Management Division

B-279842

May 18, 1998

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

As a result of rapid growth in computer technology, the Department of State, like other governmental and private sector entities, has become extremely dependent on automated information systems. Much of the data stored and processed on these systems is critical to operations involving foreign affairs, economic and commercial matters, and scientific and technological issues.

Given the sensitive[1] nature of this information and its importance to our national welfare, you asked us to determine how susceptible the State Department's unclassified automated information systems are to unauthorized access, identify what the State Department is doing to address information security issues, and determine what additional actions may be needed. We issued a classified report to you detailing the results of our review in March 1998. This is an unclassified version of that report. It summarizes the problems State faces in securing its information systems, the steps State has underway to address problems, and our recommendations for additional actions.

Results in Brief

State's information systems and the information contained within them are vulnerable to access, change, disclosure, disruption or even denial of service by unauthorized individuals. We conducted penetration tests to determine how susceptible State's systems are to unauthorized access and found that we were able to access sensitive information. In addition, we could have performed system administration actions that would have allowed us to download, delete, and modify these data, add new data, shut down servers,[2] and monitor network traffic. Moreover, our penetration of

[1] According to the Computer Security Act of 1987 (Public Law 100-235), sensitive information is "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled" under the Privacy Act of 1974, as amended. The Privacy Act requires federal agencies to keep personal information about individuals confidential.

[2] Servers are network computers that perform selected processing operations for computer users on a network.

State's computer resources went largely undetected, further underscoring the department's serious vulnerability.

The results of our tests show that individuals or organizations seeking to damage State operations, commit terrorism, or obtain financial gain could possibly exploit the department's information security weaknesses. For example, by accessing State's systems, an individual could obtain sensitive information on State's administrative processes and key business processes including diplomatic negotiations and agreements.

Although State has some projects underway to improve security of its information systems and help protect sensitive information, it does not have a security program that allows State officials to comprehensively manage the risks associated with the department's operations. First, State lacks a central focal point for overseeing and coordinating security activities. Second, State does not routinely perform risk assessments to protect its sensitive information based on its sensitivity, criticality, and value. Third, the department's primary information security policy document is incomplete. Fourth, State is not adequately ensuring that computer users are fully aware of the risks and responsibilities of protecting sensitive information. Fifth, the department lacks key controls for monitoring and evaluating the effectiveness of its security programs and it has not established a robust incident response capability.

Clearly, State needs to greatly accelerate its efforts and address these serious information security weaknesses. However, to date, its top managers have not demonstrated that they are committed to doing so. For example, despite reporting mainframe computer security as a significant weakness confronting the agency to the Congress and the President since 1987, managers have not yet developed a comprehensive security plan or ensured that adequate resources are devoted to strengthening controls and ensuring that they remain effective on a continuing basis.

Internet security was the only area in which we found that State's controls were currently adequate. However, plans to expand its Internet usage will create new security risks. State conducted an analysis of the risks involved with using Internet more extensively, but has not yet decided how to address the security risks of additional external connectivity or the concerns this review raised. If State increases its Internet use before instituting a comprehensive security program and addresses the additional vulnerabilities unique to the Internet, it will unnecessarily increase the risks of unauthorized access to its systems and information.

Background

State relies on a variety of decentralized information systems and networks to help it carry out its responsibilities and support business functions, such as personnel, financial management, medical, visas, passports, and diplomatic agreements and communications. The data stored in these systems is sensitive enough to be attractive targets for individuals and organizations seeking monetary gain or desiring to learn about or damage State operations. For example, much of this information deals with State employees and includes American and Foreign Service National personnel records, employee and retiree pay data, and private health records. Background investigation information about employees being considered for security clearances is also processed on State's unclassified network as is sensitive financial and procurement information.

The potential consequences of misuse of this information are of major concern. For example, unauthorized deletion or alteration of data could enable dangerous individuals to enter the United States. In addition, personnel information concerning approximately 35,000 State employees could be useful to foreign governments wishing to build personality profiles on selected employees. Further, manipulation of financial data could result in over- or underpayments to vendors, banks, and individuals, and inaccurate information being provided to agency managers and the Congress.

Objectives, Scope, and Methodology

Our objectives were to (1) determine how susceptible the State Department's automated information systems are to unauthorized access, (2) identify what the State Department is doing to address information security issues, and (3) determine what additional actions may be needed. To determine how susceptible State's systems are to unauthorized access, we tested the department's technical and physical controls for ensuring that data, systems, and facilities were protected from unauthorized access. We tested the operation of these controls to determine whether they existed and were operating effectively. We contracted with a major public accounting firm to assist in our evaluation and testing of these controls. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported. During our testing, we performed controlled penetration attacks at dial-in access points, the department's Internet gateways, and public information servers. We also performed penetration activities to access security controls on State's major internal networks. In addition, we performed social engineering[3] activities to assess user awareness, and attempted to gain physical access to two State facilities.

We attempted to access State's sensitive data and programs under conditions negotiated with State Department officials known as "rules of engagement." These rules were developed to assist us in obtaining access to State's facilities and information resources and to prevent damage to any systems or sensitive information. Under the rules, all testing was required to take place within the department's headquarters building between 8:00 a.m. and 10:00 p.m. and was physically monitored by State employees and contractor personnel. In addition, State monitors were authorized to stop our testing when we obtained access to sensitive information or systems. We were also required to inform State personnel about the types of tests we planned to conduct prior to the testing. As agreed with State, we limited the scope of our testing to unclassified systems.

To identify what State is doing to address the issue of unauthorized access to its information systems, we discussed with department officials their efforts to protect these systems and reviewed supporting documentation. For example, we obtained information on the department's initiatives to improve the security of its mainframe computers and establish a centrally managed information system security officer program at headquarters. We also discussed with department officials preliminary plans to expand the use of the Internet and reviewed supporting documentation. We reviewed numerous evaluations of information security at domestic State locations and foreign posts performed by the department's Bureau of Diplomatic Security. We reviewed recent reports submitted by State to the President and the Congress under provisions of the 1982 Federal Managers' Financial Integrity Act,[4] which outlined known information management and technology weaknesses and plans for corrective actions. We reviewed the department's policy guidance on information security as contained in the Foreign Affairs Manual, Volume 1 and Volume 12, Chapter 600, and its Fiscal Year 1997-2001 Strategic and Performance Management Plan for Information Resources Management. We visited a computer security

[3] Social engineering is a technique commonly used by attackers to bypass an organization's existing physical and logical security controls to gain unauthorized access to systems, networks, and resources by relying on information provided by naive, poorly trained, and well intended organizational personnel.

[4] The Financial Managers' Financial Integrity Act requires that the head of each executive agency provide an annual statement to the President and the Congress stating whether the systems of internal accounting and administrative control fully comply with standards issued by the Comptroller General.

assessment center in Fairfax, Virginia, which the department uses primarily for certifying and accrediting software to be used on State information systems.

To evaluate State's security program management and formulate recommendations for improvement, we compared State's practices to guidelines in two National Institute of Standards and Technology (NIST) publications, the "Generally Accepted Principles and Practices for Securing Information Technology Systems" and "An Introduction to Computer Security: The NIST Handbook," as well as other guides and textbooks. In addition, we reviewed a Department of State Inspector General report on unclassified mainframe systems security. We also relied on our work to identify the best information security management practices of non-federal organizations which is presented in our Executive Guide Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-21 Exposure Draft, November 1997). The guide identifies key elements of an effective information security program and practices which 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.

We performed our audit work primarily at State Department headquarters offices from July 1996 through August 1997 in accordance with generally accepted government auditing standards.

Information Systems Are Vulnerable to Unauthorized Access

Our penetration tests revealed that State's sensitive but unclassified information systems can be easily accessed by unauthorized users who in turn can read, delete, modify, or steal sensitive information on State's operations. First, while simulating outside attackers without knowledge of State's systems, we were able to successfully gain unauthorized access to State's networks through dial-in connections to modems.[5] Having obtained this access, we could have modified or deleted important data, shut down services, downloaded data, and monitored network traffic such as e-mail and data files.

We also tested internal network security controls and found them to be inadequate. For example, we were able to gain privileged (administrator) access to host systems on several different operating platforms (such as UNIX and Windows NT). This access enabled us to view international

[5] A modem is a device that enables a computer to transmit and receive information over a standard telephone line by converting digital signals into analog signals and vice versa.

financial data, travel arrangements, detailed network diagrams, a listing of valid users on local area networks, e-mail, and performance appraisals, among other sensitive data.

Our tests also found that security awareness among State employees is problematic. We were able to gain access to State's networks by guessing user passwords, bypassing physical security at one facility, and searching unattended areas for user account information and active terminal sessions. For example, in several instances we were able to enter a State facility without required identification. In an unlocked work area for one office, we found unattended personal computers logged onto a local area network. We also found a user identification and password taped to one of the computers. Using these terminals, we were able to download a file that contained a password list. In another unlocked area, we were able to access the local area network server and obtain supervisor-level access to a workstation. With this access, we could have added or deleted users, implemented unauthorized programs, and eliminated audit trails.

Our tests of dial-in-security, internal network security, and physical security demonstrated that information critical to State's operations as well as to the operations of other federal agencies operating overseas can be easily accessed and compromised. For example, we gained access to information that detailed the physical layout of State's automated information infrastructure. These data would make it much easier for an outsider who had no knowledge of State's operations or infrastructure to penetrate the department's computer resources. In addition, we obtained information on administrative and sensitive business operations which may be attractive targets to adversaries or hackers. At the conclusion of our testing, we provided senior State managers with the test results and suggestions for correcting the specific weaknesses identified.

State Lacks a Comprehensive Information Security Program

Our tests were successful primarily because State's computer security program is not comprehensive enough to effectively manage the risks to which its systems and networks are exposed. For example, the department does not have the information it needs to effectively manage its risks—it does not fully appreciate the sensitivity of its information, the vulnerabilities of its systems, or the costs of countermeasures. In addition, security is not managed by a strong focal point within the agency that can oversee and coordinate security activities. State also does not have the types of controls needed to ensure the security of its sensitive information, including current and complete security policies and enterprisewide incident reporting and response capability. Moreover, top managers at State have not demonstrated that they are committed to strengthening security over the systems that they rely on for nearly every aspect of State's operations.

Elements of a Comprehensive Security Program

Our study of information security management[6] at leading organizations identified the following five key activities that are necessary in order to effectively manage security risks.

- A strong framework with a central management focal point and ongoing processes to coordinate efforts to manage information security risks.
- Risk assessment procedures that are used by business managers to determine whether risks should be tolerated or mitigated and to select appropriate controls.
- Comprehensive and current written policies that are effectively implemented and then updated to address new risks or clarify areas of misunderstanding.
- Steps to increase the awareness of users concerning the security risks to information and systems and their responsibilities in safeguarding these assets.
- Ability to monitor and evaluate the effectiveness of policy and other controls.

Furthermore, each of these activities should be linked in a cycle to help ensure that business risks are continually monitored, policies and procedures are regularly updated, and controls are in effect.

Perhaps the single most important factor in prompting the establishment of an effective information security program is commitment from top management. Ultimately, it is top managers who ensure that the agency embraces all elements of good security and who drive the risk management cycle of activity. However, State's top managers are not demonstrating the commitment necessary to practice good security and State's information security program does not fully incorporate any of the activities described above. Specifically, there is (1) no central management focal point, (2) no routine process for assessing risks, (3) no comprehensive and current set of written policies, (4) inadequate security awareness among State personnel, and (5) no effective monitoring and evaluation of policies and controls. In addition, State lacks a

[6] Information Security Management: Learning From Leading Organizations (GAO/AIMD-98-21, Exposure Draft, November 1997).

comprehensive information security plan that would help ensure that these elements are in place.

Top Management Commitment at State Is Insufficient

While senior management at State has shown some interest in information security through actions including drafting memoranda, forming working groups to improve information security, and approving limited funding for selected security activities, this interest has not been sufficient to overcome longstanding and institutionalized security weaknesses. For example, while top management at State is aware of longstanding problems associated with its information management and information security and has reported a number of these high-risk and material weaknesses to the President and the Congress under provisions of the 1982 Federal Managers' Financial Integrity Act, these weaknesses remain unresolved. For example, mainframe computer security was identified as a material weakness 10 years ago but has not yet been corrected.

In reporting on unclassified mainframe systems security in its January 1996 Security Oversight Report, the department's Inspector General noted:

> "The lack of senior management's involvement in addressing authority, responsibility, accountability and policy is the critical issue perpetuating the Department's lax approach to mainframe security . . . . In addition, the lack of clear management responsibility has resulted in incomplete and unreliable security administration . . . ."

Many mid-level State officials told us that the information security problems we and others identified during our review were already known throughout the department. Collectively, they believed that senior State management was not convinced of the seriousness of the problems and were unable or unwilling to commit the requisite attention and resources to resolve them. They noted that budget requests for security measures, such as information systems security officers, were approved but later rescinded. Many officials said that while the assignment of a chief information officer (CIO) was a critical step in elevating the importance of information management and security throughout the department, the CIO does not have the authority needed to ensure that improvements are made throughout State's decentralized activities. They also said that budgets for important controls, such as Bureau of Diplomatic Security information security evaluations at worldwide posts, are severely constrained and that the same security deficiencies are found and ignored year after year. Other officials reported that State personnel do not carry out their security responsibilities satisfactorily because security is assigned as a low-priority collateral duty.

State Lacks a Clearly Defined Central Focal Point

The Department of State is a decentralized organization with bureaus operating semi-autonomously in their areas of responsibility. As a result, information resources management is scattered throughout the department. There is no single office responsible for overseeing the architecture, operations, configuration, or security of its networks and systems. The chief information officer, the Bureau of Diplomatic Security, and the information management office all perform information security functions. Many offices and functional bureaus also manage, develop, and procure their own networks and systems. In addition, according to Bureau of Diplomatic Security officials, some of the approximately 250 posts operated by State around the world have established their own network connections, further complicating security and configuration management.

This decentralized approach to information security is problematic. Scarce talent and resources are spread throughout the department, making communication and coordination difficult. Because the responsibilities for information security are divided among three offices, no one office is fully accountable, duties and responsibilities have been fragmented, and the department's principal security and information technology managers have often disagreed over strategy and tactics for improving the information security of the department. Perhaps most importantly, the department cannot determine if its systems are being attacked or if its information is being tampered with. State's Internet Risk Analysis states the following:

> "Since there is no enterprise-wide authority for ensuring the confidentiality, integrity and availability of information as it traverses the unclassified network, it is extremely difficult to detect when information is lost, misdirected, intercepted or spoofed. Therefore, a post that is not expecting to receive information will not miss critical information that never arrives. More importantly, if a post does receive information it was not expecting, there is no office to confirm that the transmission was legitimate and not disinformation sent by a network intruder or disgruntled employee."

State Does Not Routinely Assess Risks

In assessing risks, managers should consider the (1) value and sensitivity of the information to be protected, (2) vulnerabilities of their computers and networks, (3) threats, including hackers, thieves, disgruntled employees, competitors, and in State's case, foreign adversaries and spies,

(4) countermeasures available to combat the problem, and (5) cost-effectiveness of the countermeasures. In addition to providing the basis for selecting appropriate controls, results obtained from risk assessments should also be used to help develop and update an organizations's security plan and policies.

We met with representatives from the Office of Information Management and Bureau of Diplomatic Security who told us that they are unaware of any significant risk management activity related to information security within the department. These officials stated that they have not been requested to provide technical assistance to program managers at State. One significant exception to this is the comprehensive risk analysis performed by the Bureau of Diplomatic Security, which evaluated the risks associated with Internet connectivity.

Computer security evaluations performed at posts located around the world by Bureau of Diplomatic Security staff further demonstrate that State officials are not addressing and correcting risks appropriately. The evaluations revealed numerous problems at foreign posts such as use of inappropriate passwords and user identifications, failure to designate an information systems security officer, poor or nonexistent systems security training, and lack of contingency plans. Diplomatic security staff also told us that they have found that some posts have installed modem connections and Internet connections without approval, further complicating the department's ability to manage and secure its networks. Annual analyses of these evaluations show a pattern in which system security requirements are continually overlooked or ignored. Diplomatic security staff noted that the majority of the security deficiencies that they found are correctable with modest capital outlay and more attentive system administration.

State's Information Security Policies Are Incomplete

State's information security policies are primarily contained in its Foreign Affairs Manual. State also provides policy guidance in other formats, including instructions, cablegrams, letters, and memoranda. These policies are deficient in several respects. First, they fail to acknowledge some important security responsibilities within the department. For example, while the security manual details responsibilities of system managers and information systems security officers, it does not address the information security responsibilities of the Department's chief information officer (CIO). The CIO's authority and ability to operate effectively would be enhanced with departmental policy recognition of the legislatively prescribed security responsibilities.[7] State's Foreign Affairs Manual was updated in February 1997 to describe the CIO position, but it does not discuss any information security responsibilities.

Second, the Foreign Affairs Manual does not require and consequently provides no mandate for, or guidance on, the use of risk assessments. As previously discussed, the department does not routinely assess and manage its information security risks. There is no specific State policy requiring threat and vulnerability assessments, despite their known value.

Third, State's policy manual does not sufficiently address users' responsibilities. For example, the manual does not emphasize that users should be accountable for securing their automated data, much as they are held responsible for securing classified paper documents. And it does not adequately emphasize the importance of information and computer resources as critical assets that must be protected. A significant finding in the department's Internet risk analysis is that users and even systems administrators "do not feel that their unclassified data is sensitive and therefore spend little to no effort in protecting the data from external disclosure." Clearly stated policy and effective implementation could contribute greatly to increased awareness.

State Is Not Adequately Promoting Awareness

Often, computer attacks and security breakdowns are the result of failures on the part of computer users to take appropriate security measures. For this reason, it is vital that employees who use a computer system in their day-to-day operations be aware of the importance and sensitivity of the information they handle, as well as the business and legal reasons for maintaining its confidentiality and integrity. In accepting responsibility for security, users need to follow organizational policies and procedures, and acknowledge the consequences of security violations. They should also devise effective passwords, change them frequently, and protect them from disclosure. Further, it is important that users not leave their computers, workstations, or terminals unattended, and log out when finished using their computers. In addition, users should help maintain physical security over their assigned areas and computer resources.

[7] Under the Paperwork Reduction Act of 1995 (Public Law 104-13, Chapter 35 of Title 44, United States Code) and the Clinger-Cohen Act of 1996 (Public Law 104-106, the National Defense Authorization Act for Fiscal Year 1996), chief information officers are responsible for ensuring agency compliance with privacy and security requirements. Specifically, they are to provide advice and assistance to senior agency officials to ensure that the information security policies, procedures, and practices of their agency are adequate.

Many computer users at State had weak passwords that were easily guessed, indicating that they were unaware of or insensitive to the need for secure passwords. During our testing of State's systems, we were able to guess passwords on a number of machines on various networks using both manual guessing and automated password cracking programs. One way to prevent password guessing is to ensure that users use complex passwords such as those composed of alphanumeric, upper- and lower-case characters. However, there was no evidence that State was training its users to employ these techniques. We also found little evidence that State was training its users to prevent unauthorized access to information. For example, we called a user under the pretense that we were systems maintenance personnel and were able to convince her to disclose her password.

We also bypassed physical security at a State facility and searched unattended areas for user account information and active terminal sessions. For example, in several instances we were able to enter a facility without the required State identification by using turnstiles designed for handicapped use. Once inside the facility, we entered unlocked work areas and found unattended personal computers logged onto a local area network. From one of these computers, we downloaded a file that contained a password list. We also noticed that a password and user identification code were taped to the desk in a workstation.

State Does Not Regularly Evaluate Its Controls

Some key controls are not in place at State to ensure that it can defend its sensitive information and systems. For example, State has very little departmentwide capacity to respond to security incidents and individual bureaus currently handle incidents on an ad hoc basis. Problems experienced are not shared across the department because the incidents are not reported or tracked centrally and very little documentation is prepared. Furthermore, State does not regularly test its systems and network access controls through penetration testing. Finally, State has limited ability to visit all its worldwide locations to perform security evaluations.

Our study of information security management at leading organizations found that an organization must monitor and evaluate its policies and other controls on a regular basis to periodically reassess whether it is achieving its intended results. Testing the existence and effectiveness of controls and other risk reduction efforts can help determine if they are operating effectively. Over time, policies and controls may become inadequate because of changes in threats, changes in operations, or deterioration in the degree of compliance.

Because breaches in information security, computer viruses, and other related problems are becoming more common, an aggressive incident response capability is an important control and a key element of a good security program. Organizations need this capability to respond quickly and effectively to security incidents, help contain and repair any damage caused and prevent future damage. In recognition of the value of an incident response capability, federal agencies are now required by the Office of Management and Budget to establish formal mechanisms to respond to security incidents.[8] Many organizations are now setting up emergency response teams and coordinating with other groups, including the Federal Computer Incident Response Capability and Carnegie Mellon's Computer Emergency Response Team. Knowing that organizations have a formidable response capability has proved to be a deterrent to hackers and other unauthorized users.

State acknowledges that it needs the capability to detect and react to computer incidents and information security threats in a timely and efficient manner. At the time of our review, Department personnel were drafting incident response procedures. Bureau of Diplomatic Security officials told us that they are beginning to develop an incident response capability at the laboratory that they use to evaluate and accredit systems and software. Information management officials also told us that efforts were underway to obtain some services from the Federal Computer Incident Response Capability[9] that would help them detect and react to unauthorized access to their systems.

As discussed earlier, Bureau of Diplomatic Security performs evaluations of field locations to identify and make recommendations for correcting security weaknesses. However, Bureau of Diplomatic Security officials told us that budget constraints limit their ability to perform these evaluations and visit all locations on a systematic and timely basis. State officials also told us that they need to periodically assess the

[8] The February 1996 revision to Office of Management and Budget Circular A-130, Appendix III, Security of Federal Automated Information Systems, requires agencies to establish formal incident response mechanisms and awareness training of these mechanisms for employees.

[9] The Federal Computer Incident Response Capability is a collaboration among the National Institute of Standards and Technology, the Defense Advanced Research Project Agency's Computer Emergency Response Team Coordination Center, and the Department of Energy's Computer Incident Advisory Capability. This service has been designed to provide federal civilian agencies with cost-reimbursable, direct technical assistance and incident handling support.

vulnerabilities of and threats to their systems. They also acknowledged the need for and importance of developing a reporting mechanism that can be used across the department to share information on vulnerabilities and incidents.

An additional control mechanism that could help State ensure that controls are in place and working as intended, and that incident response capability is strong, is the annual financial statement audit. This audit is required to be conducted annually by the Chief Financial Officers Act of 1990.[10] A part of this audit could involve a detailed examination of an agency's general and application computer controls.[11] We have been working with the department's inspector general to ensure that State's financial audit includes a comprehensive assessment of these controls. When this audit is complete, management will be able to better gauge its progress in establishing and implementing sound information security controls.

State Lacks a Comprehensive Information Security Plan

Federal agencies are required by the Computer Security Act to develop and implement security plans to protect any systems containing sensitive data. The February 1996 revision to Appendix III of OMB Circular A-130 requires that a summary of the security plans be incorporated into an agency's strategic information resources management plan. State has no information security plan. Instead, the department's IRM Strategic and Performance Management Plan includes several pages of text on information security and its implementation. This discussion highlights the development of computer security and privacy plans for each system containing sensitive information, as required by the Computer Security Act. However, when we requested copies of these individual plans, we were told that they could not be located and that even if they were found, they would be virtually useless because they were drafted in the late 1980s, never updated, and are now obsolete.

The strategic plan also references other efforts underway within the department, including assessments of various software applications to identify vulnerabilities and evaluations of antivirus software products. However, this discussion is insufficient. It merely lists a set of ad hoc and

[10] The Chief Financial Officers Act of 1990 (Public Law 101-576), as amended in 1994, requires State and 23 other federal agencies to prepare financial statements that can pass the test of an independent audit and provide decisionmakers with reliable financial information.

[11] Our Federal Information System Controls Audit Manual provides guidance for evaluating general and application controls over the integrity, confidentiality, and availability of data maintained in computer-based information systems.

largely unrelated programs and projects to improve information security. It does not relate these programs to any risk-based analysis of threats to and vulnerabilities of the department's networks or systems. Furthermore, this discussion mentions the existence of but does not endorse or discuss planned efforts to implement any key recommendations identified in the Internet Risk Analysis.

A companion document to the strategic plan, the department's February 1997 Tactical Information Resources Management Plan, indicates the lack of emphasis that information security receives. According to this plan, the department should closely monitor and centrally manage all information resource management initiatives that "are critical to the Department missions; will cost more than $1 million through their life cycle; have schedules exceeding one year; and cut across organizational lines." However, the plan acknowledges that "at this time the Department has no Security projects that meet the criteria" above. In addition, the plan ignores the need for centralized management for information technology projects and, instead, requires individual offices to fund and manage their own security requirements.

Greater Internet Connectivity Poses Additional Risks

Internet security was the only area in which we found that State's controls were currently adequate. We attempted to gain access to internal State networks by going through and around State's Internet gateways or exploiting information servers from the outside via the Internet, but we were not able to gain access to State's systems. State's protection in this area is adequate, in part, because the department has limited its use and access to the Internet. However, State officials have been requesting greater Internet access and the department is considering various options for providing it.

Expansion of Internet services would provide more pathways and additional tools for an intruder to attempt to enter unclassified computer resources and therefore increase the risk to State systems. Recognizing this, State conducted an analysis of the risks involved with increasing Internet use. However, the department has not yet decided to what extent it will accept and/or address these new risks. Until it does so and implements a comprehensive security program that ensures that top managers are committed to enforcing security controls and users are fully aware of their computer security responsibilities, State will not be in a good position to expand its Internet use.

Conclusions

Networked information systems offer tremendous potential for streamlining and improving the efficiency of State Department operations. However, they also greatly increase the risks that sensitive information supporting critical State functions can be attacked. Our testing demonstrated that State does not have adequate controls to protect its computer resources and data from external attacks and unauthorized activities of trusted users who are routinely allowed access to computer resources for otherwise legitimate purposes. These weaknesses pose serious risk to State information and operations and must be mitigated.

We recognize that no organization can anticipate all potential vulnerabilities, and even if it could, it may not be cost-effective to implement every measure available to ensure protection. However, State has yet to take some basic steps to upgrade its information systems security and improve its position against unauthorized access. These steps include ensuring that top managers are fully aware of the need to protect State's computer resources, establishing a strong central management focal point to remedy the diluted and fragmented security management structure, and addressing the risks of additional external connectivity before expanding its Internet usage. Until State embraces these important aspects of good computer security, its operations, as well as those of other federal agencies that depend on State, will remain vulnerable to unauthorized access to computer systems and data.

Recommendations

We reaffirm the recommendations we made in our March 1998 classified report. These recommendations called on State to take the following actions.

- Establish a central information security unit and assign it responsibility for facilitating, coordinating, and overseeing the department's information security activities. In doing so,
  - assign the Chief Information Officer the responsibility and full authority for ensuring that the information security policies, procedures, and practices of the agency are adequate;
  - clarify the computer security responsibilities of the Bureau of Diplomatic Security, the Office of Information Management, and individual bureaus and diplomatic posts; and
  - consider whether some duties that have been assumed by these offices can be assigned to, or at a minimum coordinated with, the central information security unit.

- Develop policy and procedures that require senior State managers to regularly determine the (1) value and sensitivity of the information to be protected, (2) vulnerabilities of their computers and networks, (3) threats, including hackers, thieves, disgruntled employees, foreign adversaries, and spies, (4) countermeasures available to combat the problem, and (5) cost-effectiveness of the countermeasures.
- Revise the Foreign Affairs Manual so that it clearly describes the legislatively-mandated security responsibilities of the Chief Information Officer, the security responsibilities of senior managers and all computer users, and the need for and use of risk assessments.
- Develop and maintain an up-to-date security plan and ensure that revisions to the plan incorporate the results obtained from risk assessments.
- Establish and implement key controls to help the department protect its information systems and information, including
  - periodic penetration testing to identify vulnerabilities in State's information resources;
  - assessments of the department's ability to (1) react to intrusion and attacks on its information systems, (2) respond quickly and effectively to security incidents, (3) help contain and repair any damage caused, and (4) prevent future damage, and
  - central reporting and tracking of information security incidents to ensure that knowledge of these problems can be shared across the department and with other federal agencies.
- Ensure that the results of the annual financial statement audits required by the Chief Financial Officers Act of 1990 are used to track the department's progress in establishing, implementing, and adhering to sound information security controls.
- Require department managers to work with the central unit to expeditiously review the specific vulnerabilities and suggested actions we provided to State officials at the conclusion of our testing. After the department has reviewed these weaknesses and determined the extent to which it is willing to accept or mitigate security risks, assign the central unit responsibility for tracking the implementation and/or disposition of these actions.
- Direct the Assistant Secretary for Diplomatic Security to follow-up on the planned implementation of cost-effective enhanced physical security measures.
- Defer the expansion of Internet usage until (1) known vulnerabilities are addressed using risk-based techniques and (2) actions are taken to provide appropriate security measures commensurate with the planned level of Internet expansion.

Agency Comments and Our Evaluation

The Department of State provided written comments on a draft of our classified report and concurred with eight of our nine recommendations. In summary, State said that its Chief Information Officer is beginning to address the lack of a central focus for information systems security through the establishment of a Security Infrastructure Working Group; agreed to formalize and document risk management decisions; agreed to revise provisions of the Foreign Affairs Manual related to information security and undertake an evaluation of one of its most significant networks based on our review; and said it is implementing a plan to correct the technical weaknesses identified during our testing. State also took steps to minimize unauthorized physical access to a State facility.

State did not concur with our recommendation to defer the expansion of Internet usage. In explaining its nonconcurrence, State asserted that

- expanded use of Internet resources is a priority;
- the Chief Information Officer, Office of Information Management, and Bureau of Diplomatic Security are coordinating on architecture and security functionality that should mitigate any significant security vulnerabilities through the use of a separate enclave;
- segmenting the network, implementing controlled interfaces, restricting services, restricting the processing or transmission of sensitive unclassified information, and proactive network monitoring and incident handling should mitigate these risks; and
- a formal risk analysis of expanding the Internet throughout the department has been conducted and known risk factors are being considered in the Internet expansion.

Some of these assertions are invalid; the rest do not fully address our recommendation. First, designating expanded Internet usage as a priority does not mean that State should proceed before it fully implements appropriate security controls. If State expands Internet connectivity without effectively mitigating the significant additional risks that entails, it will increase its already serious vulnerabilities to individuals or organizations seeking to damage State's operations, commit terrorism, or obtain financial gain.

Second, State does not explain how "coordination on architecture and security functionality" between the Chief Information Officer, Office of Information Management, and Bureau of Diplomatic Security will reduce Internet risks, including computer attacks from those wishing to steal information or disable the department's systems. As noted in this report, the organizations cited by State share various information security responsibilities, but have different missions and interests. This assertion does not address our recommendation that State establish an organization unit with responsibility for and authority over all information security activities, including protecting the department from computer attacks via Internet.

Third, State identified a number of controls with it believes will reduce Internet security risks, including establishing a (logically) separate network (enclave) dedicated to Internet usage, and proactively monitoring the network and handling incidents. If effectively implemented and maintained, these measures can help reduce security risks. However, State did not specify how it planned to implement these controls, what resources it has allocated to these efforts, or if they would be completed before State expands its Internet usage. Our point is that State must actually implement and maintain security measures to mitigate these risks prior to increasing Internet usage.

Finally, we discussed State's risk analysis of expanded Internet usage in our report. This analysis identifies numerous risks associated with expansion and options for addressing them. It is not sufficient that "known risk factors are being considered in the Internet expansion"; as previously noted, State must mitigate these risks prior to increasing Internet usage.

As agreed with your offices, unless you publicly announce the contents of this report earlier, we will not distribute it until 30 days from its date. At that time, we will send copies of this report to the Chairman and Ranking Minority Members of the House Government Reform and Oversight Committee, Senate Committee on Appropriations, Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, the House Committee on Appropriations, Subcommittee on Commerce, Justice, State, the Judiciary and Related Agencies, and the Secretary of State. Copies will be available to others upon request.

If you have questions about this report, please contact me at (202) 512-6240. Major contributors are listed in appendix I.

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

Major Contributors to This Report

Accounting and Information Management Division, Washington, D.C.

Keith A. Rhodes, Technical Director
John B. Stephenson, Assistant Director
Kirk J. Daubenspeck, Evaluator-in-Charge
Patrick R. Dugan, Auditor
Cristina T. Chaplain, Communications Analyst

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are $2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

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

or visit:

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

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

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

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

info@www.gao.gov

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

http://www.gao.gov

PRINTED ON ♻ RECYCLED PAPER

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

Official Business
Penalty for Private Use $300

Address Correction Requested