United States General Accounting Office

GAO

Testimony

Before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate

For Release at
10 a.m.
Tuesday,
February 1, 2000

CRITICAL INFRASTRUCTURE PROTECTION

Comments on the National Plan for Information Systems Protection

Statement for the Record by
Jack L. Brock, Jr., Director
Governmentwide and Defense Information Systems
Accounting and Information Management Division

Mr. Chairman and Members of the Subcommittee:

I am pleased to be here today to discuss the *National Plan for Information Systems Protection*.[1] This plan calls for new initiatives to strengthen the nation's defenses against threats to public and private sector information systems that are critical to the country's economic and social welfare, particularly those supporting public utilities, telecommunications, finance, emergency services, and government operations. As a "preliminary" document, it is intended to begin a dialogue on its proposals and lead to the development of plans for protecting other elements of the nation's infrastructure, including those pertaining to the physical infrastructure and specific roles and responsibilities for state and local governments and the private sector.

Beginning this dialogue is vital. As I stressed at this Subcommittee's October 1999 hearing[2] on critical infrastructure protection, our nation's computer-based infrastructures are at increasing risk of severe disruption. The dramatic increase of computer interconnectivity–while facilitating communications, business processes, and access to information–has increased the risk that problems affecting one system will also affect other interconnected systems. Massive computer networks provide pathways among systems that, if not properly secured, can be used to gain unauthorized access to data and operations from remote locations. While the threats or sources of these problems can include natural disasters, such as earthquakes, and system-induced problems, government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

This plan is an important and positive step forward toward building the cyber defense necessary to protect critical information assets and infrastructures.

- It identifies risks associated with our nation's dependence on computers and computer networks for critical services.

- It recognizes the need for the federal government to take the lead in addressing critical infrastructure risks and to serve as a model for information security.

[1] *Defending America's Cyberspace: National Plan for Information Systems Protection: Version 1.0: An Invitation to a Dialogue.* Released January 7, 2000. The White House.

[2] *Critical Infrastructure Protection: Fundamental Improvements Needed to Assure Security of Federal Operations* (GAO/T-AIMD-00-7, October 6, 1999).

- It outlines key concepts and general initiatives to assist in achieving these goals.

In doing this, the plan addresses many of the same points we raised at last October's hearing, including the need for improved standards, strengthened evaluations and oversight of agency performance, increased technical expertise, adequate funding, and improved incident detection and response capabilities.

However, there are opportunities for improvement as the plan is further developed as well as significant challenges that must be addressed to build the public-private partnerships necessary for infrastructure protection. In particular, we believe the plan should place more emphasis on providing agencies the incentives and tools to implement the management controls necessary to assure comprehensive computer security programs, as opposed to its current strong emphasis on implementing intrusion detection capabilities. In addition, the plan relies heavily on legislation and requirements already in place that, as a whole, are outmoded and inadequate as well as poorly implemented by the agencies.

Mr. Chairman, my testimony today will provide a more detailed overview of the plan, identify opportunities for sharpening the plan's proposals for improving the federal government's security programs, and outline the challenges facing the government in building the public-private partnerships necessary for comprehensive infrastructure protections.

Overview of the National Plan for Information Systems Protection

The *National Plan for Information Systems Protection* is intended as a first major element of a more comprehensive effort to protect the nation's information systems and critical assets from future attacks. This preliminary version focuses largely on federal efforts being undertaken to protect the nation's critical cyber-based infrastructures. Subsequent versions are to address a broader range of concerns, including the specific role industry and state and local governments will play in protecting physical and cyber-based infrastructures from deliberate attack as well as international aspects of critical infrastructure protection. The end goal of this process is to develop a comprehensive national strategy for infrastructure assurance as envisioned by Presidential Decision Directive (PDD) 63.[3]

The plan proposes achieving its twin goals of making the U.S. government a model of information security and developing a public-private partnership to defend our national infrastructure through the following 10 programs which are intended to serve three crosscutting infrastructure protection objectives.

Table 1: Infrastructure Protection Objectives and Programs

Crosscutting Objective		Program
Prepare and Prevent	The steps necessary to minimize the possibility of significant and successful attack on our critical information networks, and build an infrastructure that remains effective in the face of such attacks.	Identify critical infrastructure assets and shared interdependencies and address vulnerabilities.
Detect and Respond	The actions required to identify and assess an attack in a timely way, and then to contain the attack, quickly recover from it, and reconstitute affected systems.	Detect attacks and unauthorized intrusions. Develop intelligence and law enforcement capabilities to protect critical information systems. Share attack warning and information in a timely manner. Create capabilities for response, reconstitution, and recovery.
Build Strong Foundations	The steps needed to create and nourish the people, organizations, laws, and traditions that will make us better able to prepare for and prevent, detect, and respond to attacks on our critical information networks.	Enhance research and development. Train and employ adequate numbers of information security specialists. Outreach to make Americans aware of the need for improved cyber security. Adopt legislation and appropriations to support infrastructure protections. Ensure the full protection of American citizen's civil liberties, their rights to privacy, and their rights to the protection of proprietary data.

[3] Issued in May 1998, this directive requires that the Executive Branch assess the cyber vulnerabilities of the nation's critical infrastructures—information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health, as well as those authorities responsibility for continuity of federal, state, and local governments. The directive places special emphasis on protecting the government's own critical assets from cyber attack and the need to remedy deficiencies in order to become a model of information security.

Making the Federal Government a Model

Making the federal government a model of good information security is essential to the plan’s success. However, the gap between expectations and actual agency performance is significant. As we testified last October and in subsequent written responses to your questions,[4] our government is not adequately protecting critical federal operations and assets from computer-based attacks. In particular, recent audits conducted by GAO and agency inspectors general show that 22 of the largest federal agencies have significant computer security weaknesses, ranging from poor controls over access to sensitive systems and data, to poor control over software development and changes, and nonexistent or weak continuity of service plans.

Importantly, our audits have repeatedly identified serious deficiencies in the most basic controls over access to federal systems. For example, managers often provided overly broad access privileges to very large groups of users, affording far more individuals than necessary the ability to browse, and sometimes, modify or delete sensitive or critical information. In addition, access was often not appropriately authorized or documented; users often shared accounts and passwords or posted passwords in plain view; software access controls were improperly implemented; and user activity was not adequately monitored to deter and identify inappropriate actions.

While a number of factors have contributed to weak federal information security, such as insufficient understanding of risks, technical staff shortages, and a lack of system and security architectures, the fundamental underlying problem is poor security program management. As we reported in 1996 and, again, in 1998,[5] agencies have not established security management programs to ensure that controls, once implemented properly, are effective on an ongoing basis. This framework of effective access controls and management oversight is fundamental to any good computer security program.[6]

[4] *Responses to Posthearing Questions* (GAO/AIMD-00-46R, November 30, 1999).

[5] *Information Security: Opportunities for Improved OMB Oversight of Agency Practices* (GAO/AIMD-96-110, September 24, 1996) and *Information Security: Serious Weaknesses Place Critical Federal Operations and Assets at Risk* (GAO/AIMD-98-92, September 23, 1998).

[6] To identify potential solutions to this problem, we studied the security management practices of eight nonfederal organizations known for their superior security programs. We found that these organizations managed their information security risks through a cycle of risk management activities. The basic framework, built on 16 specific practices, allows risk management through an ongoing cycle of activities coordinated by a central focal point. See *Information Security Management: Learning From Leading Organizations* (GAO/AIMD-98-68, May 1998).

At last October's hearing, we also observed that other crosscutting actions–ranging from clarifying the roles and responsibilities of the many entities involved in information security, to strengthening oversight, to securing adequate technical expertise and funding–were needed in seven key areas to provide greater assurance that critical infrastructure objectives can be met. I would like to discuss how the plan addresses each of these areas and what additional actions need to be taken.

Clearly Defined Roles and Responsibilities

It is important that a federal strategy delineate the roles and responsibilities of the numerous federal entities involved in information security and related aspects of critical infrastructure protection. Under current law, OMB is responsible for overseeing and coordinating federal agency security; and the National Institute of Standards and Technology (NIST), with assistance from the National Security Agency (NSA), is responsible for establishing related standards. In addition, interagency bodies, such as the CIO Council and the entities created under PDD 63, are attempting to coordinate agency initiatives. However, the proliferation of organizations with overlapping oversight and assistance responsibilities is a source of potential confusion among agency personnel and may be an inefficient use of scarce technical resources.

The plan takes some positive steps to resolve this problem. For example, it discusses in very general terms how tasks associated with accomplishing the plan's objectives relate to computer security responsibilities outlined in existing laws and related guidance. These include the federal computer security and information resource management responsibilities of OMB, agency Chief Information Officers, Chief Financial Officers as well as the CIO Council. It describes OMB's core responsibility for managing federal computer security and information technology. And it generally defines the roles of the major entities created by PDD 63, including the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, the Critical Infrastructure Assurance Office, and the National Infrastructure Protection Center.

In this regard, the plan makes a start at better defining the critical infrastructure protection responsibilities of the many federal entities involved. The plan also introduces or formalizes a number of new entities, interagency working groups, and projects that will have to be integrated into the existing framework of computer security activities. Examples of these new entities and efforts include an Expert Review Team for evaluating agency infrastructure protection plans, a Federal Intrusion Detection Network, and an interagency working group on system security practices. Because of the number of entities involved (some established by law, some by executive order, and others with less formal mandates), strong and effective leadership will be essential to ensure that their efforts are coordinated and adequately communicated to individual agency personnel and that critical infrastructure protection efforts are appropriately linked with broader computer security efforts.

Risk-Based Standards

The plan recognizes the need for improved standards and asserts that NSA, NIST, GSA, and OMB will work together to identify or develop recommended practices and standards for critical federal information systems. The plan further states an intent to encourage adoption of a uniform set of standards throughout government and private industry. While on the surface these appear to be commendable goals, they do not recognize that such standards must be tailored to provide for varying levels of protection. As the plan is further developed, its focus needs to be sharpened to provide such recognition.

Currently, agencies have wide discretion in deciding (1) what computer controls to implement and (2) the level of rigor with which to enforce these controls. In theory, this is appropriate since, as OMB and NIST guidance states, the level of protection provided should be commensurate with the related risk to operations and assets. In security, one size does not fit all. The risks associated with different types of data and operations vary, depending on their sensitivity and criticality. For example, for undercover law enforcement operations, data confidentiality must be protected at all cost, while for other types of data, such as current information on financial markets, data integrity is the uppermost concern.

Our audit work has shown that agencies have generally done a very poor job of evaluating their information security risks and implementing appropriate controls. As a result, we believe that more specific guidance on what types of controls are appropriate for specific types of systems and data and the ways in which these controls should be implemented would be helpful. Specifically, a more prescriptive set of control standards, supported by a range of data classifications and related minimum requirements, would help clarify expectations for information protection, provide a framework for assessing information security risk, and help ensure that similar types of data and shared data are provided the same level of protection from one agency to another. In essence, risk-based standards would assist agencies in ensuring that their most critical operations and assets are protected at the highest levels, while providing agencies the flexibility to apply less rigorous (and often less expensive and less cumbersome) controls to lower-risk operations and assets.

Routine Evaluations of Agency Performance

Agency managers have a responsibility to not only determine the level and type of controls necessary to protect information assets but also to routinely evaluate those controls to assess their effectiveness. This responsibility is not being met. At present, there is no mechanism for routinely testing and evaluating the effectiveness of agency information security programs and presenting the results in a way that is meaningful to agency managers.[7] In addition, there is no standard testing methodology that is applied consistently from year to year and among organizations. Without such mechanisms, there is no reliable and meaningful way to measure agency information security practices and, in turn, to provide OMB and the Congress with the information needed to gauge agency performance and hold agencies accountable for implementing needed improvements.

The plan takes some constructive steps in this regard. Particularly, it calls on federal agencies to put in place programs to carry out several types of vulnerability testing and analysis, including routine automated system configuration/integrity/vulnerability testing using commercial-off-the-shelf tools, regular internal self-assessments, and independent external critical reviews. At an agency's request, NSA and NIST are to perform independent analyses of critical federal information infrastructure and provide independent reports of their results to the agency's CIO. And, as mentioned earlier, the plan anticipates establishing a permanent Expert Review Team at NIST to assist governmentwide agencies in adhering to federal computer security requirements.[8]

Nevertheless, we believe that the plan's provisions for testing agency controls may not be rigorous enough. Tests initiated by agency officials are essential because they provide information needed to fulfill their ongoing responsibility for managing security programs. However, routine in-depth tests and evaluations initiated by independent auditors, such as agency inspectors general, are also critical because they serve as an independent check on management evaluations and provide reliable information on actual control effectiveness for congressional and executive branch oversight.

Our audits at individual agencies and our best practices work have shown that a continuous cycle of testing, reassessment of risk, and adjustments to policies and controls is needed to ensure that efforts to protect

[7] Some independent testing of systems is done through agency annual financial statement audits.

[8] The Critical Infrastructure Assurance Office first established expert review teams in November 1998 to evaluate agency critical infrastructure assurance plans.

information remain appropriate and effective on an ongoing basis. Establishing such a cycle of activity will require a significant commitment by agency management, the federal audit community, and federal centers of technical expertise, such as NSA and NIST. It will be important for any new audit requirements, including those associated with the Expert Review Team, to be conducted in this context.

Executive Branch and Congressional Oversight

Having effective oversight over agency performance is the linchpin to maximizing protection over critical infrastructure and assets. The government’s recent success in dealing with the Year 2000 issue demonstrated the impact that good oversight–both in the Congress and within the agencies–coupled with performance objectives and performance data can have on effective program management. Those success factors are lacking in cyber protection. There is too little incentive for agencies to adhere to guidance, too little performance data to promote truly effective oversight, and too little effort among those providing oversight to exert corrective action.

The administration’s call to action through this plan’s development and increased congressional interest indicates a heightened concern over cyber security and provides a basis for increased oversight. As noted in the previous section, initial oversight must provide a heavy focus on agency management’s fulfillment of its obligations to set and evaluate meaningful controls over its information environment.

Adequate Technical Expertise

Federal agencies cannot provide needed information security without trained staff. The Computer Security Act authorized NIST to provide assistance to agencies and included provisions for periodic training in computer security awareness and practice. However, the availability of adequate technical expertise has been a continuing concern to agencies. GAO has not specifically analyzed the technical skills of agency personnel involved in computer security across government. But we have observed a number of instances where agency staff did not have the skills needed to carry out their computer security responsibilities and were not adequately overseeing activities conducted by contractors. As technology evolves, the challenge of training and retaining people with the expertise to select, implement, and maintain computer security controls is likely to increase.

The plan does a good job of addressing this issue. It describes a program to develop a cadre of highly skilled computer science and information security personnel. This program, if implemented, would include estimating personnel and training needs; establishing centers for information technology excellence that will provide web-based and classroom information security training to federal employees, college and high school students; initiating a scholarship program under which recipients would agree to a pre-determined commitment to federal government service; and establishing a high school and secondary school outreach program.

Adequate Funding

Federal agencies must have adequate resources to support their information security and infrastructure protection efforts. Funding for security is already embedded to some extent in agency budgets for computer system development efforts and routine network and system management and maintenance. However, some additional amounts are likely to be needed to address specific weaknesses and new tasks.

In releasing the plan on January 7, the President announced that he was proposing a 16 percent increase in funding for critical infrastructure protection in his fiscal year 2001 budget proposal. To jumpstart fiscal year 01 initiatives, the President also proposed $9 million in supplemental funding for this spring.

We have not had the opportunity to examine this proposal in detail. However, as this plan evolves, it will be important to secure OMB and congressional oversight of spending in order to ensure that expenditures are targeted toward reducing the most significant risks and that controls implemented are effective. Our audits have shown that, in the past, agencies have expended resources on controls that, when tested, proved to be ineffective. In addition, they have often addressed identified weaknesses in an ad hoc, piecemeal fashion that resulted in limited improvement. It will be important for future security budgets to be based primarily on risk-based needs and for expenditures be evaluated, to the extent possible, in terms of actual risk reduction.

Incident Detection and Response

Given the vast scale and variety of federal operations, there is a pressing need to more comprehensively monitor and develop responses to intrusions, viruses, and other incidents that threaten federal systems. Several entities are already providing some central coordination and guidance in this area—including the FBI, NIST, and the FedCIRC.[9] However, as noted in our previous testimony, the specific roles and responsibilities of these organizations, as well as the balance between

[9] FedCIRC—the Federal Computer Incident Response Capability—is a reporting center at the General Services Administration.

governmentwide and individual agency responsibilities, should be clarified and expanded to provide a more comprehensive picture of the security events that are occurring and assistance in dealing with them.

The plan proposes to strengthen incident detection and response by developing mechanisms for regular sharing of federal threats, vulnerability, and warning data; and sponsoring conferences to further the coordination and development of common operating systems. In particular, it calls for a governmentwide system for analyzing and correlating attack data consisting of three elements: one for the Department of Defense and national security communities (the Joint Task Force-Computer Network Defense, which is already deployed), a second for non-Defense federal departments and agencies (the Federal Intrusion Detection Network, or FIDNet which will build on existing DOD and other security technology expertise), and a third that provides information to both systems (the National Security Incident Response Center, or NSIRC, which has already been deployed to provide expert assistance to the national security community in isolating, containing, and resolving incidents threatening national security systems).

We agree that developing improved intrusion detection and response capabilities is important. However, available tools and methods for analyzing network traffic and detecting intrusions are still evolving and cannot yet be relied on to serve as an effective “burglar alarm,” as envisioned by the plan. While holding promise for the future, such tools and methods currently raise many questions regarding technical feasibility, cost-effectiveness, and the appropriate extent of centralized federal oversight. Accordingly, these efforts merit close congressional oversight.

Legislative Framework

As noted earlier, one of our major concerns with the plan is that it relies on current law, policies, and practices, which are based largely on the Computer Security Act of 1987, even though the act is outmoded and inadequate, as well as poorly implemented. This is a fundamental problem for several reasons. First, the act focuses too much attention on individual system security, rather than taking an organizationwide perspective. Such a narrow focus is unworkable in a networked environment. Second, the act oversimplifies risk considerations by implying that there are only two categories of information: sensitive versus nonsensitive or classified versus nonclassified. As a result, it fails to recognize that security must be managed for a range of varying levels of risk to the integrity, availability, and confidentiality of information supporting agency operations and assets. Third, the act treats information security as a technical function, rather than as a management function, which removes security from its integral role in program management. Lastly, the Computer Security Act does not require an evaluation of implemented controls (i.e., no testing). And, while OMB’s computer security guidance provides more complete guidance and calls for testing of agency controls, we believe a more rigorous routine audit process is needed as well as a more prescriptive set of risk-based minimum mandatory standards for agencies to follow.

At present, there is legislation pending in both Houses that seeks to correct some of these underlying deficiencies. Among other things, these proposals call for a more comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support federal operations and assets; recognize the highly networked nature of the federal computing environment; and provide better oversight mechanisms. Such efforts could play an integral role in further strengthening the plan.

Engaging Public-Private Partnerships

The second facet of the plan focuses on developing a public-private partnership to protect our nation’s infrastructure. In doing so, the plan proposes developing mechanisms and improving incentives for the private sector to cooperate voluntarily with the federal government, as well as with state and local governments, to work together to provide for the common defense of the infrastructure.

For instance, the plan seeks to establish a Partnership for Critical Infrastructure Security and a National Infrastructure Assurance Council to increase corporate and government communications about shared threats to critical information systems. It also proposes establishing Information Sharing and Analysis Centers to facilitate public-private sector information sharing about actual threats and vulnerabilities in individual infrastructure sectors. These, as well as other proposals, however, are presented in broad terms, with the intent that future versions of the plan will describe a full spectrum of specific actions and programs that have been jointly agreed upon by industry and all levels of government.

We believe this approach is reasonable given the formidable challenges involved in developing effective partnerships with the private sector. The plan itself recognizes some of these challenges. For example, it acknowledges that critical infrastructure protection is not exclusively, even largely, within the province of the federal government, and, as a result, the federal government is limited in what it can do to protect critical infrastructures. It also recognizes that while the nature of the threat to our national infrastructure has changed, the true extent of that threat, our vulnerability to it, and possible means of defense are not entirely clear. Furthermore, the plan appreciates that solutions to critical infrastructure protection must be tailored sector by sector, through consultation about vulnerabilities, threats, and possible response strategies.

At the same time the plan recognizes such challenges, it proposes several initiatives that may have a significant impact on the private sector and affected interest groups. For example, the plan raises the possibility of reviewing laws for possible amendments to remove barriers that discourage private sector companies from sharing information with government agencies about infrastructure protection issues. Specifically, it raises the idea of more explicit confidentiality protections (so that federal law enforcement or defense agencies could assure private companies that such information would not be accessible through the Freedom of Information Act) as well as changes to antitrust or tort liability laws. Because such changes could involve important tradeoffs among significant policy concerns as well as affected interest groups, it will be important to proceed carefully in addressing the concerns of affected parties while at the same time providing the incentives needed to garner private sector cooperation.

The plan also suggests increasing employer rights to monitor employees. This would provide one means of protecting organizations from the “insiders,” who as a practical matter, probably pose a greater threat to organizational security than do external threats. Again, the challenge will lie in balancing individual privacy concerns with the need to protect sensitive assets and the common welfare.

These are just two examples of possible changes that may have the potential of improving the public-private partnership for information protection, but that will require extensive public dialogue before they could or should be implemented.

Mr. Chairman, this concludes my statement. The plan fulfills the commitment made on its title page: it does invite a meaningful dialogue. The plan is an engaging step forward in improving the nation’s cyber infrastructure. As noted in the statement, much more needs to be done to strengthen the plan’s ambitious goal of making the government a model. And serious consideration of changes in the computer security legislative framework is necessary to better assure agency compliance with good practice and process. Finally, the challenges facing the establishment of a meaningful public-private partnership require a level of continuous, longterm commitment on all sides that will be difficult to sustain but that are certainly achievable.

(511693)