V Information Age Insecurity

The Information Age is irrevocably altering the means by which the Government must approach the challenge of protecting its information. Protection no longer equates to placing documents in filing cabinets with strong combination locks. Instead, information vital to the security and continued prosperity of the United States resides in a series of increasingly interconnected classified and unclassified systems. The Commission believes that the findings and recommendations noted below provide policymakers the means to begin protecting information properly now and into the next century.

This is an era of extraordinary change not only in information technology, but also in the very way in which individuals communicate with one another. The Commission's goal is not to predict the future that these technological changes will help mold. Rather, it is to better understand the nature of the new threats, so that the Government, with the full support of the private sector, can mitigate or prevent them.

At present, there exists what appears to be a growing gap between technological change and the human capacity to adapt to that change. The risk is that the Government will make bad decisions not because it has too little information, but rather because it has too much information about the wrong things. In such a rapid-paced and changing environment, it is only natural to fall back on old biases, protocols, and shortcuts. Convictions, as Nietzsche once noted, can be "more dangerous enemies of truth than lies."

Federal Government Information Security and the National Information Infrastructure

The information revolution, characterized by the growing convergence of computer and communications technologies, requires a fundamental rethinking of traditional approaches to safeguarding national security information. Those responsible for the protection of national security face new, increasingly difficult challenges presented by the proliferation of computer networks linked by telephone lines, cable, direct broadcast service, and wireless communications, and by the replacement of the traditional computer mainframe by personal computers. In this new electronic world—the National Information Infrastructure (NII)—best symbolized by the steadily growing global Internet, it is not clear what responsibility the Federal Government has to protect the infrastructure that stores, carries, and transmits nearly all of the Government's unclassified and classified information.

The NII within the United States is only one portion of the Global Information Infrastructure (GII) that connects public and private computer networks around the world. For the Federal Government to assume a leadership position in protecting the NII,

which is critical both to maintaining economic security and to promoting electronic commerce, would require the dedication of significant resources and effort.

While government involvement in protecting the nation's information infrastructure today is limited, the Preamble to the Constitution makes clear that its citizenry expects government to have a responsibility and means "to insure domestic tranquility [and] provide for the common defense." Even a partial disruption of America's critical infrastructures would, by any account, erode "domestic tranquility." A major incentive for increased government responsibility for protection of the National Information Infrastructure is the degree of reliance by both the civilian and military sectors of government on the infrastructure to carry vital communications, both classified and unclassified.

Both the NII and the GII are evolving at an exponential pace, and there appears to be little agreement concerning how best to shape their development, as well as a lack of existing institutions capable of leading such an effort. Standards for protecting and managing information systems contained within the NII do not currently exist. Furthermore, there is no visible national forum that exists to promote consistent and coordinated international cooperation in defining protection needs or standards, nor is there any comprehensive legislative framework for protecting information and information systems that addresses the variety of perspectives representing law enforcement, national security, the commercial sector, and privacy interests.

Moore's Law

"In 1965 Gordon Moore, who later co-founded Intel, predicted that the capacity of a computer chip would double every year. He said this on the basis of having examined the price/performance ratio of computer chips over the three previous years and projecting it forward. In truth, Moore didn't believe that this rate of improvement would last long, but ten years later his forecasting proved true. And then he predicted the capacity would double every two years. To this day, his predictions have held up, and the average—a doubling every 18 months—is referred to among engineers as Moore's law."

Bill Gates, *The Road Ahead*

The Commission has identified four critical means for improving information systems security: (1) greater Executive Branch oversight and accountability; (2) increased congressional oversight and accountability; (3) improved education, awareness, and training; and (4) upgraded capabilities for responding to new and emerging threats. These are discussed following a review of why the Government must take the lead in enhancing information systems security.

Source: *The Los Angeles Times*, December 10, 1974. Reprinted with permission of *The Los Angeles Times*.

The Growing Threat to Information Systems Security

Information technology costs for the Federal Government exceeded $25 billion in 1995. Within its civilian agencies, the Government employed 120,000 information technology workers, and operated 25,000 medium and large mainframe computers and more than two million individual work stations.[1] The Department of Defense has over two million computers, 10,000 local area networks, and 100 long-distance networks. The civilian sector has a critical responsibility to maintain privacy and services for the public using automated data processing and relying on the National Information Infrastructure. Just as critical to the Department of Defense is its ability to carry out any mission that is dependent on information carried on and supported by the NII. If key responsibilities of both the civilian and military sectors of government are heavily dependent upon an unsecured, potentially unavailable Internet, the Government must address whether this reliance on the NII (and GII) is acceptable and, if so, how to manage the risks involved.

Notwithstanding considerable expenditures on information technology, there exists a widening chasm between the security requirements of and the protection provided for unclassified systems government-wide and those applied to the classified systems that are located principally within the Defense and Intelligence Communities. For example, in the civilian sector, the integrity and availability of information are primary concerns; however, in the Defense and Intelligence Communities, the confidentiality of information has been the traditional concern. Thus, the Executive Branch justifiably remains reluctant to impose upon unclassified networks a classified information systems security standard of confidentiality, primarily because of additional costs and other administrative burdens.

The NII itself is vulnerable to many disruptive forces, including natural events, mistakes, technical failures, and malicious acts. For example:

> A lightning strike on a critical node in a network may cause node failure; an earthquake or hurricane may not only physically disrupt the network but also cause network congestion, another source of disruption. . . . Cutting a fiber optic cable with a backhoe may result in the loss of a primary telecommunications link. A power failure at a critical network node may cause a significant loss of data and information and may isolate portions of the network. Corrupting of key network management data by a network manager can cause many networks to fail. Viruses introduced by [adversaries domestic or foreign] can cause a network to become overloaded and ineffective or to break down at a critical juncture.[2]

The disruptive nature of such occurrences, however caused, was demonstrated in 1988, when a self-replicating software "worm" was released into the Internet and infected over 6,000 host computers worldwide in less than two hours. By the year 2000, it is estimated that the Internet will have 250 million users worldwide operating on 96 million host computers. The potential threat posed by such growth will be a major source of concern, particularly to the Defense Department, which is using the NII to improve its information sharing and its communications connectivity.

Malicious Data & Computer Security

"Traditionally, computer security focuses on containing the effects of malicious users or malicious programs. As programs become more complex, an additional threat arises: malicious data. . . . In general, the outlook is depressing: as the economic incentives increase, these vulnerabilities are likely to be exploited more frequently."

W. Olin Sibert, 19th National Information Systems Security Conference (October 1996)

The General Accounting Office (GAO) has pointed out the national security threat implicit in the relatively inexpensive advantages provided to potential enemies by Internet connections.[3] Disruptions of military operations or denial of service from critical communications nets and power systems to a deploying or deployed U.S. expeditionary force could be the "electronic Pearl Harbor" that some have been forecasting. Nor does the threat emanate only from potential "conventional" information warfare foes. Terrorism has the potential to greatly damage any society that is increasingly dependent on electronic means of creating, storing, and disseminating most or all of its information. The terrorist threat has multiple potential targets, all of which are "on-line," including the Department of Defense, government agencies, private industry, health care organizations, airlines, stock markets, banks, and law enforcement agencies.

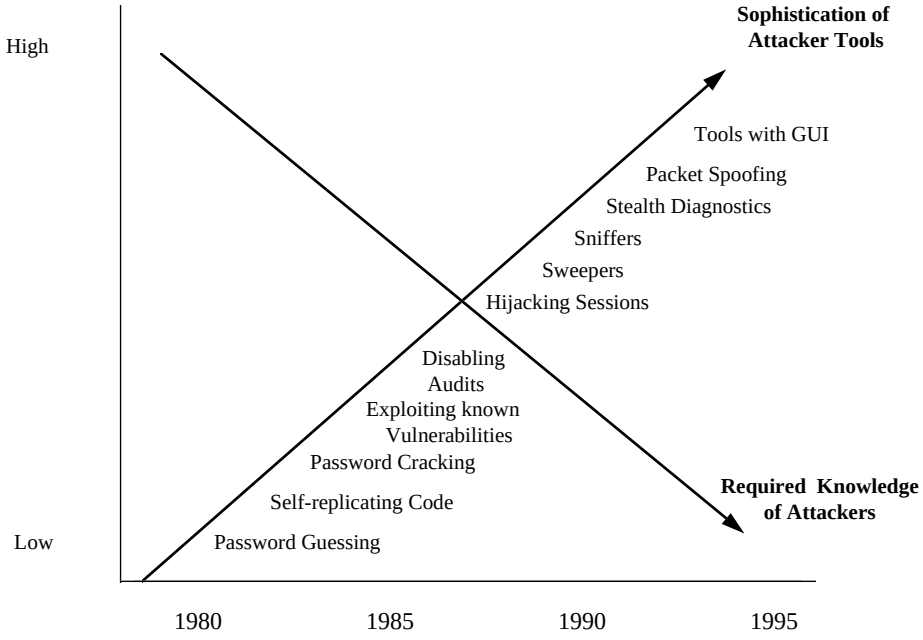
Given the costs of damage that has been caused by mere "hackers" in the way of fraud, theft, and denial of accurate information, the threat posed by "cyber terrorists" cannot be dismissed. As Professor Walter Laqueur wrote in a Spring 1996 article in *Foreign Affairs*, the difference between the range of threats posed by hackers on the one hand, and cyber terrorists on the other, is that the latter have the will and the capabilities to destroy or render unusable the NII.

However, being on-line does not necessarily imply a universal vulnerability. Those who understand security and use it effectively also are growing in numbers and sophistication. Many new and evolving defensive tools are available already and more will become available once the private sector becomes more cognizant of emerging threats and the need to better protect information systems, especially when conducting electronic commerce.

Commercial telecommunications carriers, part of the Public Network and, in turn, part of the NII, provide over 95 percent of the DoD's worldwide telecommunications needs.

The range of threats to national information systems is well catalogued. The National Institute of Standards and Technology (NIST) lists threats and associated losses based on their prevalence and significance in the current computing environment and their expected growth.[4] The GAO noted in its May 1996 report (Figure 6) that the sophistication of attacker tools is increasing while the required knowledge of the attackers is decreasing.[5] The Department of Justice and the FBI estimate that while only ten percent of the criminal community was computer literate in 1996, this rate will climb to 70 percent by 2010.[6] According to the National Research

Figure 6: Trends in Hacker Tools



Source: Defense Information Systems Agency, Briefing to Commission staff, March 21, 1996.

Council report of May 1996, "Of all the information vulnerabilities facing U.S. companies internationally, electronic vulnerabilities appear to be the most significant." The report identifies four principal threat sources to U.S. businesses: "Foreign national agencies (including intelligence services); disgruntled or disloyal employees that work 'from the inside'; network hackers and electronic vandals; and thieves."[7]

In December 1995, the President's National Security Telecommunications Advisory Committee assessed the risks to the nation's Public Network (PN), which includes any switching system or voice, data, or video transmission system that is used to provide communications services to the public, noting that ". . . computer intruders are using increasingly advanced software tools and techniques to attack the PN; . . . the PN is the means for providing access to other desirable targets; . . . and the PN is rapidly evolving to incorporate many different emerging technologies and services, and additional security standards are needed."[8]

The Improving Federal Response

The increased threat to national information systems has not gone unnoticed by the Executive Branch and the Congress. In July 1996, President Clinton issued Executive Order 13010, "Critical Infrastructure Protection," which established the Commission on Critical Infrastructure Protection to study the threats to and develop national policy for protecting critical infrastructures. The Commission will present its findings by July 1997. The Order also created an interim Information Protection Task Force, chaired by the FBI, "to identify and coordinate existing expertise, inside and outside the

Federal Government … in order to coordinate existing infrastructure protection efforts to better address and prevent crises that [will] have a debilitating regional or national impact."[10]

The Subcommittee on Investigations of the Senate Committee on Governmental Affairs, at the urging of former Senator Sam Nunn, held a series of hearings in May, June, and July 1996 regarding the threats to and potential solutions for protecting the NII. Government and industry officials, together with Members of Congress, proffered opinions for identifying and countering both existing and emerging threats. The Subcommittee also heard testimony regarding Executive Order 13010.

Despite past and continuing problems, recent Executive Branch initiatives demonstrate that information systems security is becoming a primary national security concern. For example, on July 16, 1996, Deputy Secretary of Defense John P. White testified before the Senate Government Affairs Committee's Permanent Subcommittee on Investigations regarding security in cyberspace. In the course of his testimony, he described a proposal to create a Joint Defense and Intelligence Community Information Warfare Technical Center that would be located at the National Security Agency. The Center would have the "responsibility to bring the expertise of the intelligence and military communities to define common problems and provide community-specific solutions that will contribute further to information and infrastructure assurance through employment of advanced technology."[11] The Commission believes that centers such as this one could serve as bridges to industry to garner their support in solving this burgeoning problem.

The Federal Government attempts to balance two important and often conflicting policy objectives when dealing with information systems security: (1) promoting the development and widespread use of cost-effective information safeguards, and (2) controlling the proliferation of technologies that might impair national security and law enforcement capabilities. Until the arrival of computers, these protective methods or safeguards took the form of secret codebooks, passwords, and seals to authenticate signatures. Today's world of electronic recording, storing, and transmittal features the mathematical analogues of these systems. The most successful of these safeguards are based on cryptography, which is the technique of concealing the contents of a message by code or cipher.

In 1992, the Computer System Security and Privacy Advisory Board, established by the Department of Commerce pursuant to the Computer Security Act of 1987, recommended a broad national cryptographic policy review before any new or additional cryptographic solution is approved as a U.S. Government standard.[12] The following year the Board noted that any approved standard must address issues of national security and law enforcement protection, the protection of commercial sector computer and telecommunications interests, and the protection of individual liberty interests. It also stated that "the Congress of the United States must be involved in the establishment of cryptographic policy." More recently, the Board endorsed the May 1996 National Research Council's *CRISIS* report, which found that the primary problem in dealing with cryptography is a policy vacuum: to date it has proven impossible to develop a consensus for a coherent national cryptography policy.

Currently, the United States is in an information protection quandary, best exemplified by the ongoing debate regarding cryptography and the commercial export of strong encryption algorithms. The existing national protection standard, developed by the Department of Commerce in 1977, is the Data Encryption Standard (DES). The DES is a published Federal encryption standard, developed jointly with industry, that is used to protect unclassified computer data and communications.

The DES certification period as the Federal Information Protection Standard expires in 1998, with no apparent "public" algorithm alternative in sight. However, the NIST is initiating a process that is intended to lead to the selection of an encryption algorithm for government use as an eventual successor to the DES. While there is no prohibition on the use of DES within the United States, under current export control laws it may not generally be exported by U.S. firms as part of a computer's operating system. The most notable exception is its exportability to financial organizations worldwide.

Until recently, the Executive Branch had failed to develop a new plan for protecting information transmitted across electronic systems. This failure was based on the setback experienced with the rejection of the "Clipper Chip" proposal in 1994 that would have permitted the decoding of encrypted data by U.S. Government officials if warranted by law enforcement or national security concerns. However, on November 15, 1996, the President issued Executive Order 13026, entitled "Encryption Export Policy." This new policy removes encryption products from the U.S. Munitions List regulated by the Department of State, and places them on the Commerce Control List of the Department of Commerce.[13] Although not fully embraced by industry, this policy change is designed to encourage global adoption of a key recovery system and development of a key management infrastructure, as well as allow for the use of strong encryption while protecting public safety and national security.

Improving Oversight Mechanisms

Enhancing Executive Branch Oversight and Policy Formulation

A chief shortcoming in any effort to address the range of important information systems security issues is the persistent lack of effective Executive Branch oversight and the consequent scarcity of resources devoted to information systems security. The Executive Branch lacks centralized focus and direction in developing oversight mechanisms for protecting both unclassified and classified data in Federal information systems, and for ensuring that the development of technology necessary to provide security for information systems keeps pace with the development of the systems technology itself.

The Commission believes that more focused oversight, coupled with better guidance from key components of the Government, would improve the current situation. There is no department of information or information security to oversee the government information infrastructure, much less the national information infrastructure. There is no information technology official equivalent to the Surgeon General to advise the public and government officials alike of the perils from the latest strains of "cyber-diseases." There is no Information Systems Security "911" to call when any number

of problems could arise. There is no single policy formulator within the Executive Branch for information systems security. Inspector General offices, with few exceptions, lack the personnel, skills, and resources to address and oversee information systems security within their respective agencies. The President cannot turn to an "Information General" and ask how U.S. investments in information technology are being protected from the latest viruses, terrorists, or hackers.

Over the last ten years, a convoluted information systems security policymaking structure has developed. The Computer Security Act of 1987 and the subsequent National Security Directive (NSD) 42 divided the responsibility for information systems security between the classified and unclassified worlds. If, however, the objective of the 1987 Act was to develop a clear system of policy development and oversight, the result has been just the opposite. In this confusing system, merely ascertaining the correct total number of computer units requiring protection within the Federal Government has proven problematic.

The NIST's Computer Security Division in its Computer Systems Laboratory is charged with developing standards and guidelines for unclassified information systems security, but it has been given relatively few resources to complete this task. In addition, the OMB should wield considerable authority in its role of enforcing information resources management policies and accounting for security in information technology procurement by civilian agencies. However, with only limited resources devoted to this task, the OMB has been unable to effectively monitor agency compliance with either legislative or regulatory requirements.

For classified information systems, policymaking is bifurcated. The Security Policy Board (SPB) reports to the President through the Assistant to the President for National Security Affairs. The National Security Telecommunications and Information Systems Security Committee, created under NSD 42, reports to a Steering Group consisting of fourteen heads of various departments and agencies, each having significant interaction with national security information systems. Both have policymaking responsibilities. The SPB has been unable to create a formal interagency committee structure for discussing information technology issues, largely because it focuses primarily on security issues dealing with classified information within Defense and the Intelligence Community. Information systems security concerns all branches of the Government, and the private sector as well. A previous attempt by the SPB in December 1994 to address sensitive but unclassified information met with great resistance by both the civilian side of the Government and industry.

There are additional examples that illustrate the diffusion of policymaking responsibilities. The Defense Department has the responsibility for implementing policies and procedures for protecting classified information systems. The Director of the National Security Agency is responsible for performing sixteen different tasks, the most significant of which involve: (1) providing technical assistance in protecting classified information systems; (2) upon request, providing assistance in protecting unclassified information systems; and (3) coordinating research and development of techniques and equipment to secure national security systems. The Director of Central Intelligence creates overall guidelines for the Intelligence Community.

In September 1993, the Clinton Administration created several new organizations in an attempt to shape both the development and the security of the NII. These groups included the Information Infrastructure Task Force and its subset, the NII Security Issues Forum, as well as the U.S. Advisory Council on the National Information Infrastructure and its security working group. The work of the Task Force is coming to a close, and the U.S. Advisory Council issued its last report in March 1996.

However, the Task Force report of September 1995 failed to address organizational issues, resources, policy, proposed legislation, and authorities for the agencies to act in protecting the NII. Although the groups have succeeded in generating public discussion of information systems security issues, critics from industry allege that their efforts have been chaotic, disorganized, and lacking in direction. The Commission received comments from the private sector urging that policy development in this area, including the best means of protecting sensitive unclassified information in automated information systems, should be guided by a group located outside the Defense and Intelligence Communities, in light of the fact that approximately 90 percent of all government information is not classified.[14] Such a group would need the authority to develop new rules and policies governing information systems security. (For further discussion of sensitive but unclassified information see Chapter II.)

Table 3: Potential Legislative Jurisdiction for Information Systems Security

Senate Committees
- Committee on Appropriations
- Committee on Armed Services
- Committee on Banking, Housing, and Urban Affairs
- Committee on Commerce, Science, and Transportation
- Committee on Foreign Relations
- Committee on Governmental Affairs
- Committee on the Judiciary
- Select Committee on Intelligence

House Committees
- Committee on Appropriations
- Committee on Banking and Financial Services
- Committee on Commerce
- Committee on International Relations
- Committee on Government Reform and Oversight
- Committee on the Judiciary
- Committee on National Security
- Committee on Science
- Permanent Select Committee on Intelligence

Enhancing Congressional Oversight and Policy Formulation

There will be no substantive, long-term improvements in security policy without a unifying structure to provide leadership, focus, and direction on information systems security matters.[15] The Congress should play a key role in developing such a policy. As discussed both in the 1995 Office of Technology Assessment report and in the May 1996 report of the National Research Council, the Congress has vital roles to play in areas such as cryptographic policy, safeguarding of information, protecting personal privacy in a network-based society, and reform of export control laws.

However, as Table 3 shows, a diverse array of committees and subcommittees have potential responsibility for information systems security issues. The Congress, therefore, appears poorly organized at present to assist in formulating policy and conducting effective oversight in this area. Partly as a result of this lack of a clear structure, the Congress has failed to develop overarching policy and guidance that ensure sufficient focus and direction on these and other important information security issues.

In addition to these organizational problems, the existing legislative framework for computer security issues is badly outdated. That framework, the Computer Security

Act of 1987, was enacted before the proliferation of connectivity and networked personal computers. The Act called for improving the security and protecting the privacy of sensitive information in Federal computer systems, and it created a means for establishing minimum acceptable security practices for such systems. As noted above, it also provided that protection of classified information systems is the responsibility of the NSA, leaving responsibility for unclassified information with the Commerce Department's NIST. However, the Act failed to provide the NIST with the resources or authority needed to accomplish its mandate. For example, the NIST has never received adequate funding and other support needed to pursue projects to stimulate greater systems security among civilian agencies.

The Computer Security Act of 1987, by maintaining clear lines of authority between classified and unclassified information systems and by assigning responsibilities to separate bureaucracies, failed to foresee today's world of computer connectivity and the threats posed to and by that world. Now, a decade later, the Act should be revised to reflect the realities of today's Information Age and to provide a focal point for a comprehensive effort to implement a national information infrastructure policy that takes account of the numerous and complex interests at stake. An updated statutory framework could also help replace the disparate regulations and legislative proposals that have emerged over the past decade. The reallocation of existing resources to safeguard national information systems properly should be accompanied by a clarification of the threats faced by the civilian parts of the Federal Government.

Recommendation

The Commission recommends revising the Computer Security Act of 1987 to reflect the realities of information systems security in the Information Age.

Some of the changes to the Act might include:

- Moving the Computer Systems Laboratory from the NIST to a higher visibility position within the Commerce Department, thereby increasing the likelihood of funding and personnel to support the civilian side of Government;
- Directing agencies to set aside specific funds, perhaps as a budget line item, for information systems security training; and
- Requiring the Office of Personnel Management to create a career path for information systems security professionals that includes network administration and computer crime investigation.

As with the Executive Branch, promising recent developments reflect heightened Congressional attention to the above concerns. For example, beginning in May 1996, the Senate's Permanent Subcommittee on Investigations held a series of hearings to focus on information systems security. The Subcommittee assembled panels of

high-ranking government officials and private sector experts to attest to the weaknesses and vulnerabilities of both government and private sector information systems. In addition, the GAO, at the request of the Subcommittee, submitted a report that made public the increasing vulnerabilities of unclassified Department of Defense computer systems.[16]

However, to date efforts to develop legislation in this area remain fragmented. Subjects encompassed by recent bills include encryption, copyright protection, threat assessments, criminal computer activity, and espionage through computer systems. The FY 1997 Defense Authorization Act addressed information systems security by calling for the President to submit to the Congress a "description of the national policy and plans to meet essential Government and civilian needs during a national security emergency associated with a strategic attack on elements of the national infrastructure" and to "assign responsibilities to Federal departments and agencies in the event of a strategic attack on the information systems-dependent national infrastructure."[17] The Commission believes that the initiative by the Administration, outlined in Executive Order 13010, is a good first step in response to that legislative mandate.

Addressing Current Problems

Preventing Redundancies in Technology Development

The Federal Government has no standardized mechanism for coordinating and informing agencies of technology developments. As a result, agencies often duplicate efforts and waste resources by overlooking or ignoring technological tools existing elsewhere in the Government. Although it would save money to simply adapt to one form or another, many agencies distrust the quality of products developed at other agencies, or believe that their own specialized needs require some duplication of effort. For example, the Departments of Defense and Energy each developed separate electronic personnel security questionnaires, despite knowing that all government agencies eventually will use a standardized form. The limited resource base of the future will necessitate more cooperation and free exchange of ideas and technology and less of an attitude of "not invented here."

However, there are positive signs that more cooperative research and development efforts are starting to emerge. For example, at Fort Leavenworth, Kansas, the U.S. Army, with advice from other Government organizations, has constructed an electronic records management "test bed" that incorporates many features of this cooperative approach. It is available to all Federal agencies: the Army shares insights from its experience with the test bed and offers without charge all software used in the system to any agency. This is an example of the cooperative spirit that is needed to establish a sound electronic records management structure in the Federal Government.

In addition, the Congress and the Executive Branch recently have established guidelines for developing new information systems that may impose some order on the creation of information systems security tools and avoid wasteful expenditures. However, both the Information Technology Management Reform Act and Executive Order 13011, "Federal Information Technology," fail to create a central mechanism

that coordinates the Government's focus on emerging technologies. The Commission believes that creating a central technology clearinghouse to coordinate all research and development regarding information technology and to standardize government information technology acquisitions might lessen the burden on departments and agencies. The need for this approach is already implicit within the context of Executive Order 13011.

Promoting Government-Industry Cooperation

Government and industry cooperation in the world of information technology is not a new concept. More than twenty years ago, a partnership between government and industry solved that generation's need for strong encryption with the Data Encryption Standard. At that time, the security offered by DES was sufficient for protecting sensitive unclassified information within the Government. Due to technological advances in encryption-breaking techniques, however, certain protective technologies, such as DES now are too weak to adequately protect banking and other extremely sensitive information.

With a growing national and global need for new information protection standards, government and industry must reinvigorate their partnership. Maintaining a U.S. leadership role in developing and promulgating international standards is dependent upon such cooperation both domestically and internationally. Moreover, a government oversight role in developing and promulgating safeguarding standards is highly desirable. Information systems products mutually developed by government and industry carry an implied guarantee of integrity and reliability that no private firm alone can provide.

Advocates of renewed government-industry cooperation to solve information protection problems recognize that there must be incentives, such as indemnification, in order for industry to cooperate with the Government. Information systems security problems will not be "just" government or "just" industry problems; they will be shared by all who need information protection. Only the Federal Government, however, has the resources to invest on the scale needed to ensure functioning large-scale systems and can provide the forums necessary to permit public debate on the concerns of the different equities involved: privacy, law enforcement, national security, and commercial interests.

Discouraging the Use of Classification as an Alternative to Effective Information Systems Security

Studies conducted in the last several years, including those by Defense agencies, private companies, Congressional committees, and the General Accounting Office, have shown that Federal information systems are extremely vulnerable to attacks by both foreign governments and hackers. The publicity created by these investigative efforts has heightened concern about protecting certain sensitive but unclassified data that reside on computer systems.

Because of these high-profile reports and other expressions of concern regarding unauthorized access to and potential destruction of Government information systems, some Members of Congress have suggested that sensitive information stored on computer systems should be incorporated into new or existing classification levels to provide an extra measure of protection. Classification, however, addresses the *symptoms* rather than the causes of existing problems. Extending classification to potentially millions of sensitive but unclassified documents would both be costly and run directly counter to the intent in Executive Order 12958 and other efforts to reduce the scope of classification. The Federal Government instead should work toward developing and implementing more effective and coordinated computer security measures.

Improving information systems security is preferable to and less costly than the very expensive process of classifying millions of sensitive documents that do not currently warrant such form of protection and control. This approach would require agencies to address the real problem: computer system vulnerabilities throughout the Federal Government and the inadequate response thus far.

Encouraging Greater Accountability and Leadership

In light of the more than $25 billion spent for information technology in 1995, it is reasonable to question what type and quality of information systems security the Federal Government has obtained in return for its investment. It appears clear that there has been neither adequate leadership nor accountability with respect to agency investments in information systems security technology. Under provisions of the new Information Technology Management Reform Act enacted in February 1996, Chief Information Officers at agencies are now specifically responsible for making proper decisions on technology acquisitions. With rare exceptions, however, the management of information technology resources is not specified in the job descriptions of agency heads. Nor is the required successful and comprehensive security for these assets mentioned in the job descriptions of the security officers whom senior officials may place in charge of information technology acquisitions and operations. Often, security officers are assigned to implement and oversee computer security requirements as a third or fourth additional duty.

Furthermore, the OMB has assigned only two people to oversee the entire information systems infrastructure of the Federal Government (excluding the DoD and the Intelligence Community). The NIST's Computer Systems Laboratory has 25 people and a $4 million budget to "secure" the Federal Government's unclassified information systems. There is no oversight of research and development and acquisitions among agencies to avoid redundancies and duplications. Agencies thus are left to implement their security programs with little regard for the correct mix of security required. Information systems decisionmaking is budget-driven, and security appropriations often are the first line items to be eliminated or reduced.

On the legislative side, the disparate and overlapping committee and subcommittee jurisdictions make it difficult to coordinate leadership in the Congress on matters of information systems security. Moreover, the entire world of information systems and

systems security remains unexciting to many; as a result, Members of Congress for the most part have not given it much attention.

The Congress needs an independent, focused research and analytical capability if it is to make informed judgments on the direction the Executive Branch chooses to take concerning information technology and other related issues. This is especially true when Congressional committees must exercise oversight of individual departments and agencies that are developing information resource management approaches in response to statutory requirements. Greater expertise would provide the Congress with the information necessary to make decisions on technology issues in a rapidly changing technical environment. Such expertise can be developed by using existing resources within the Congressional Research Service and the Government Accounting Office to advise the Congress on policy formulation, oversight, and other duties in the area of information technology.

Planning for the Future

The requirements of the next century will demand that the Federal Government and industry work more closely than ever before to develop technologies that address the problems that accompany the rapid proliferation of information systems within the Federal Government. Prioritizing and dedicating the necessary resources are essential in each of the areas listed below.

Disseminating Threat Information

In spite of recent attempts to facilitate and encourage broader dissemination of threat information produced by elements of the Intelligence and Law Enforcement Communities, much of the information available still is provided in paper form or through briefing of individuals. There exists no systematic means for informing government agencies or private industry about the threats to the National Information Infrastructure. Accurate and timely threat information, available on-line, could assist interested parties in focusing limited resources to counter key threats and encourage industry to provide threat information to other firms as well as to the Government.

While a fully automated threat dissemination process would place an additional burden on the Intelligence and Law Enforcement Communities, the benefits derived from such a process would far outweigh any additional costs, especially if the change encourages private industry to become a full partner in addressing the threats to the NII. However, prior to expanding the existing automated intelligence information systems to include new industry customers, current as well as potential users must be aware of and understand the concerns raised by the Intelligence Community in potentially providing certain extremely sensitive intelligence information to industry customers. With innovations such as INTELINK, an Internet-like database that contains classified information for the Defense and Intelligence Communities, this isolation of classified computer systems has begun to diminish. The costs to the Government and industry for establishing a contractor version of a database, such as INTELINK, can range from as little as $5,000 for a basic computer and secure telephone unit to $500,000 for a complete system that includes audio and video capability for Top Secret/Sensitive Compartmented Information.[18]

Increasing Awareness of Computer Attacks

At present, there is no national-level computer incident response center that is able to receive, analyze, compare, collate, and disseminate to appropriate authorities incidents of computer attack, "denial of service," or computer crime. The Commission believes that current technology offers potential means for addressing shortcomings in the detecting and reporting of computer attacks or attempted intrusions. For example, the Federal Emergency Management Agency has an existing state and local information infrastructure in place to support a national computer incident response center, thus reducing the need for substantial investment in additional bureaucracy and spending. Any effort to establish a national response center could capitalize on existing infrastructures, until such time as a clear need for a more permanent structure and reporting system emerges.

A national computer incident response center could build upon experiences gained from existing computer emergency response entities. A response center would utilize mainly existing infrastructure and lines of communication, keeping new costs down. Reporting received, including that from state and local levels, would help focus agencies on the need to manage risks and would encourage the development of a database that promotes more accurate threat assessments.

Friendly Greetings?

One company whose officials met with the Commission warned its employees against reading an e-mail entitled "Penpal Greetings." Although the message appeared to be a friendly letter, it contained a virus that could infect the hard drive and destroy all data present. The virus was self-replicating, which meant that once the message was read, it would automatically forward itself to any e-mail address stored in the recipient's in-box.

To be effective, such a center would require cooperation from the private sector as well as from state and local governments. This cooperation may be difficult to achieve, however, especially from corporations and financial institutions reluctant to acknowledge losses from computer attacks. An expressed promise of confidentiality in protecting information received from both government and nongovernment sources would be essential for private industry to provide attack information.

Developing Auditing and Intrusion Detection Capabilities

The exponential increase in computer network interconnectivity has made automated information systems simultaneously more powerful and more vulnerable to attacks or intrusions. Attempts to compromise the confidentiality, integrity, or availability of information in these systems tend to exploit flaws in either the operating system or the application programs. The degree to which these intrusions are prevented, or at least diverted, is directly related to the amount of resources and time devoted to building and maintaining the system's defenses. Improvements are needed both in detection and in the collection of data on intrusions. An intrusion detection system does not, in and of itself, stop an intrusion in progress; it merely serves as a mechanism to alert system security officials. Intrusion detection systems must be combined with timely assessment and response capabilities in order to achieve effective systems security. As stated at the National Information Systems Security Conference in October 1995:

> Computer and Internet misuse has become a frequent topic of today's mainstream media, and the demand for anti-intrusion technology is exploding. However, intrusion detection products are as yet esoteric and not well integrated to work together with complementary approaches such as intrusion preventing "firewalls."[19]

One encouraging sign is that the technological advances that have occurred since that Conference now do provide some limited means of scanning for system vulnerabilities.

An intrusion detection system must identify, preferably in real time, unauthorized use, misuse, or abuse of computer systems. More reliable data collection also would permit more reliable assessments of the dangers posed by these intrusions. One reason computer intrusions into unclassified systems are not reported within the Federal Government is that most agencies do not mandate that incidents be reported. In the private sector, there is great reluctance to report anything to the Government. These reasons include fear of loss of client base if the information is revealed; lack of indemnification by the Government for failing to protect information owned by others; and a presumptive drain on limited resources to obtain protective measures with no incentives to do so.

Just as in the private sector, many Federal agencies are reluctant to make the investments required in this area because of limited budgets, lack of direction and prioritization from senior officials, and general ignorance of the threat. Without spending mandates, managers will not prioritize in favor of protecting extremely vulnerable unclassified databases. An additional problem is that detection of intrusions in classified information systems still may not be able to eliminate the possibility of unauthorized copying of classified data. As the May 1996 GAO report on DoD intrusions stated, attacks are exploiting basic vulnerabilities such as poor password usage. Improved intrusion detection systems cannot be a cure for careless and ineffective computer security procedures or techniques.

Including Security in Automation Projects

All Federal Government agencies today are using automation, including the Internet, to increase their productivity, efficiency, and visibility to the public, and to achieve cost savings. However, at present there are few security standards available to guide agencies in creating and implementing automation projects. As a result, the degree of information security varies from project to project, sometimes leaving sensitive information susceptible to interception, duplication, or malicious alteration. In addition, most operating systems within a given computer have many security features that are not turned on automatically when the system is activated or started. These features, once activated, would markedly improve the overall security posture of the system without spending additional resources, if officials had the training and awareness to utilize the systems to the fullest extent possible.

If agencies fail to implement adequate security during the initial stages of an automation project, they may be forced to add security, usually at far greater cost and in the glare of public scrutiny, during a later crisis. Estimates in the Joint Security Commission report suggest that incorporating security into a computer system during

the planning stages costs between 5 and 10 percent of the entire project budget. In contrast, the cost can rise to 25 percent of the project's budget if security is not implemented until after problems arise, as is usually the case.[20]

Professionalizing Information Systems Security

The Federal Government must promote greater awareness of the vulnerabilities of national information systems. One way to do so is to create, support, and promote an information systems security career field within the Government. The NSA's National Computer Security Center has made significant advances in defining the knowledge, skills and abilities, curriculum requirements, and on-the-job experience required to produce information systems security specialists. Its program for developing a professional cadre to secure the classified systems can serve as a model for protecting the unclassified systems of the Government and the private sector.

Despite the need, there currently is no government-wide speciality or career field for computer security personnel, network administrators, or computer crime investigators. Nor are there any universities or colleges offering a doctoral program in Computer Security; while the NSA's National Computer Security Center is in the process of promoting such a program, it is expected to take years to fully develop.[21] Focusing more attention on the development of a computer security career path, within both the Government and the private sector, would ensure the continued presence of personnel and resources devoted to safeguarding information systems—critical in an era of increased connectivity and heightened system vulnerabilities.

Agencies should be prepared to refocus existing resources on the training needed to create information systems security specialists. The direction must come from the top for creating a career path as an incentive for improving the quality of the computer security force expertise. Senior managers and leaders must be made aware of the need for a quality force to protect national information systems and must provide the guidance, authority, and direction necessary to meet this need.

Recommendation

The Commission recommends developing an information systems security career path across the Government.

Strengthening Information Technology Training and Awareness

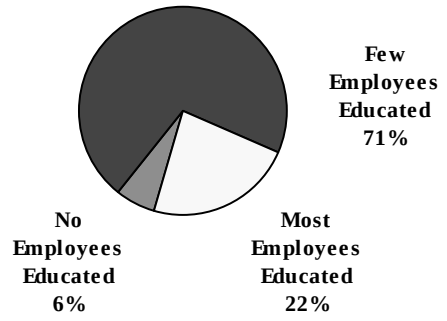
Senior Executive Branch and Congressional officials, users of Federal computers, and overseers of information systems security all need continuing education and training to remain abreast of developments in information systems technology and understand how to protect the contents of those information systems.

The first element of such education and training efforts concerns the basic rules for use of information systems. No coordinated Federal Government effort exists to teach computer ethics or rules of behavior to employees working on Federal computer systems. A 1996 survey of Federal agencies and private corporations showed that few employees even had a working knowledge of current laws on the misuse of computer systems. The results of that survey are shown in Figure 7.

A 1994 report by the Office of Technology Assessment noted that "unauthorized use of computers by authorized users is estimated to be the second largest source of computerized losses," following only human error.[22] If agencies wish to focus on the critical issue of training, automated courses on computer ethics and safeguarding would allow large numbers of government employees to receive training more cheaply than through traditional classroom instruction; recently, several government agencies have begun to develop such computerized training courses.

The second element of training focuses on security awareness. The Computer Security Act of 1987 requires agencies to improve the security and protect the privacy of sensitive information in Federal computer systems. The Act cites mandatory Federal computer security training as a means of attaining improved security awareness and accepted computer security practices. Yet despite the increased threats and vulnerabilities present in today's national information infrastructure, there is little evidence of serious attempts to increase training and education programs. The 1987 Act does not ensure that agencies budget sufficient resources to safeguard information assets, and, in reality, the training provision of the 1987 Act was an unfunded mandate.

Figure 7: Percentage of Companies with Employees Educated on Computer Abuse Laws



Source: *Computer Security Issues & Trends,* vol. II, no. 2 (San Francisco: Computer Security Institute, Spring 1996), 9.

Information exchange that is automated and accessible at low cost is the third element of security education, training, and awareness. Such information exchange must provide a communication infrastructure that reflects the technological advances of the next century. The recent efforts of the Defense Advanced Research Projects Agency (DARPA) to automate a customer-driven information exchange database are noteworthy. DARPA's experience and expertise in creating and supporting the forerunner of the Internet has served as the basis for creating a private network (Intranet) that provides security officials, both within Government and industry, such a communications link for problem solving. DARPA's know-how and objectivity in efforts such as this security-focused Intranet can help foster additional progress on information exchange.

Conclusion

The Federal Government has a clear responsibility to protect its own information infrastructure. Less clear is what the Government should be doing to protect the overall National Information Infrastructure. The transmittal of both classified and unclassified Government information depends upon the privately-created NII lines of communication, but the Government has no claim or right to control the private, commercial, and proprietary information moving across the same systems. In the event of an attack on the NII resulting in significant damage to the security of the nation as a whole, to selected elements of the population, or to critical infrastructures, policies and procedures that are well-founded and well-tested must be in place.

Leadership is lacking, however, throughout the Federal Government in the area of information systems and systems security, and as a result, agencies have not dedicated the resources needed to protect information systems adequately. If senior officials were made more aware of the magnitude of the problem and held more accountable for information systems security, the necessary prioritization of resources probably would follow.

Solutions do not lie in the creation of new government bureaucracies. In fact, many of the tools needed to create coherent policy, advise agencies, and educate system users and protectors already exist. The fact that Inspectors General do not pursue oversight of information systems security does not mean that they cannot, given greater emphasis and resources from their respective agencies' leadership. The fact that the NIST's Computer Systems Laboratory has not vigorously pursued security solutions and standards does not mean that it cannot, given dynamic leadership and the funds needed to do its work. The fact that the NSA has been viewed as a traditional protector of classified information does not mean that it cannot devote more of its considerable resources to advising about protection of the unclassified government information systems. The fact that the Computer Security Act of 1987 is ill-suited for a world of connectivity does not mean that the law cannot be amended or replaced to reflect today's needs.

In summary, the security of the Government's information systems would be enhanced as a result of increased attention in three broad areas: (1) national policy development, application, and oversight; (2) threat recognition and crisis management; and (3) professionalization of the information systems security career field. This Commission believes that the existing Presidential Commission on Critical Infrastructure Protection is ideally suited to expand upon this report's findings in the area of information technology and, through its own recommendations, to educate the Government and the public on the preferred approaches to efficient protection of information systems.

---

[1] Office of Management and Budget, "Security of Federal Automated Information Resources" (Washington, D.C., February 1996, briefing sheet), 8.

[2] Department of Defense, Joint Staff, *INFORMATION WARFARE*: *Legal, Regulatory, Policy and Organizational Considerations for Assurance*, prepared by SAIC, 2nd ed. (Washington, D.C.: Department of Defense, 4 July 1996), 2-18.

[3] General Accounting Office, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks*, GAO/AIMD-96-94 (Washington, D.C.: Government Printing Office, May 1996), 11-12.
[4] National Institute of Science and Technology, *An Introduction to Computer Security: The NIST Handbook*, 800-12 (Washington, D.C.: Government Printing Office, October 1995), 21.
[5] General Accounting Office, *Information Security*, 13.
[6] Interview by Commission Staff, 12 September 1996.
[7] National Research Council, *Cryptography's Role in Securing the Information Society (CRISIS*) (Washington, D.C.: National Academy Press, 30 May 1996), 1-25.
[8] National Security Telecommunications Advisory Committee, Network Security Information Exchange, *An Assessment of the Risk To the Security of Public Networks* (Washington, D.C.: National Communications System, December 1995), ES1-ES2.
[9] Department of Defense, Joint Staff, *INFORMATION WARFARE*: *Legal, Regulatory, Policy and Organizational Considerations for Assurance*, prepared by SAIC (Washington, D.C.: 4 July 1995), 1-1.
[10] President, Executive Order 13010, "Critical Infrastructure Protection," *Federal Register* 61, no. 138 (17 July 1996): 37345 - 37350.
[11] Senate Committee on Governmental Affairs, *Security in Cyberspace: Hearings before the Subcommittee on Investigations*, 104th Cong., 2nd sess., 16 July 1996.
[12] Office of Technology Assessment, *Information Security and Privacy in Network Environments*, OTA-TCT-606 (Washington, D.C.: Government Printing Office, 1994), 176-177.
[13] President, Executive Order 13026, "Encryption Export Policy," *Federal Register* 61, no. 224 (19 November 1996): 58767-58768.
[14] National Security Telecommunications Advisory Committee, Network Security Information Exchange, *An Assessment of the Risk to the Security of Public Networks*, 2.
[15] Joint Security Commission, *Redefining Security* (Washington, D.C.: 28 February 1994), 2, 102, 106. For further discussion on sensitive but unclassified information, see also Chapter II, pages 28-29 of the report.
[16] General Accounting Office, *Information Security*, 2.
[17] Public Law 104-201, 104th Cong., 2nd sess. (23 September 1996).
[18] Office of the Executive Director, Intelligence Community Affairs Staff, telephone conversation with Commission Staff, 4 September 1996.
[19] Lawrence R. Halme and R. Kenneth Bauer, "AINT Misbehaving — A Taxonomy of Anti-Intrusion Techniques," *Proceedings of the 18th National Information Systems Security Conference*, Vol. I (Baltimore: National Institute of Standards and Technology, 10-13 October 1995), 164.
[20] Department of Defense official, telephone conversation with Commission Staff, 30 July 1996.
[21] Department of Defense official, telephone conversation with Commission Staff, 7 June 1996.
[22] Office of Technology Assessment, *Information Security and Privacy in Network Environments*, 25-26.