Statement of
ROBERTA L. GROSS
Inspector General
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION
Before the
Senate Committee on Governmental Affairs
March 2, 2000

Mr. Chairman and members of the Committee,

I thank you for the opportunity to be here today to discuss S. 1993, the Government Information Security Act of 1999. My testimony generally will be based on the audits, reviews and criminal investigations performed by the NASA Office of Inspector General (OIG). This work provides insight into NASA's information technology (IT) security program. I also head a legislative working group reviewing S. 1993 comprised of OIG representatives from both the President's and Executive Councils on Integrity and Efficiency (PCIE/ECIE).[(1)] The group has received input from 24 members of these Councils. These representatives by and large agree that the S. 1993 is a very positive step in highlighting the importance of centralized oversight and coordination in responding to risks and threats to IT security. I will also offer comments raised by this group.

INTRODUCTION

At its most extreme, the interoperability of networks has made both our nation's and our agencies' critical infrastructures more vulnerable to intrusion and destruction. Consider NASA OIG's recent press release reporting on a joint computer crimes investigation by the NASA OIG Computer Crimes Division (CCD); the Defense Criminal Investigative Service; the Federal Bureau of Investigation; the U. S. Department of the Interior, Office of Inspector General; and the Immigration and Naturalization Service, Office of Investigations.

> On February 23, 2000, Ikenna Iffih was charged in a three-count criminal information filed in U. S. District Court in Boston… Iffih obtained unauthorized access to a dial-up Internet account. On April 10-11, 1999, Iffih used that account to compromise a Defense Logistics Agency (DLA) computer in Columbus, OH. Using the DLA computer, Iffih illegally accessed a computer owned by the Zebra Marketing Online Service (ZMOS) in Seattle, WA, and through his allegedly reckless actions, damaged that computer and caused a significant loss of revenue to ZMOS. On May 6, 1999, Iffih illegally accessed a computer located at the Goddard Space Flight Center (GSFC) in Greenbelt, MD, and used his access to install a "sniffer" program to review and capture login names and passwords transmitted on the GSFC network. Iffih then used the GSFC computer to illegally access and modify (deface) a Department of the Interior web server on May 31, 1999.
>
> On August 25, 1999, a search warrant was executed at Iffih's residence and the subsequent forensic examination of Iffih's personal computer revealed that Iffih had obtained unauthorized access to multiple computers owned and operated by Northeastern University (NEU), Boston, MA, and was in possession of personal identifying information on over 9,000 individuals associated with NEU.

Other recent headlines have made clear the vulnerability of our networked systems to malicious hackers. No one can doubt that securing information from theft, manipulation,

denial of service attacks, and alteration will be an important factor in shaping future Federal planning and investment of information resources. However, determining how much security is enough is ultimately a matter of judgment. In a world of limited budgets and competing programmatic and infrastructure priorities, each agency must determine the most critical programs and the proper security for the systems supporting those programs. For example, NASA's mission includes inspiring the public through human exploration of space. The Space Shuttle, NASA's reusable space launch vehicle, piloted and staffed by its astronauts and principal investigators, is a key component of human space exploration. The shuttle program, including research projects conducted aboard the shuttle, involves elaborate network connectivity between the NASA centers and private industries, universities, and foreign nations. NASA also provides public web sites to inform the public about its role in the human exploration of space. Obviously, the level of security needed to protect NASA public web sites is not the same as that needed to ensure astronaut safety aboard the Space Shuttle.

Further complicating network security planning is that payback from the investment in information security is uncertain. Just recall discussions in the media as to whether the Y2K[(2)] effort was hype. However, headlines would have been far different if the Government's Y2K efforts had failed. IT security failures also make headlines.

Today's hearing reflects this Committee's recognition of the importance of planning a national coordinated approach to IT security. While it is essential that the debate continue over the precise implementation of a comprehensive plan, S. 1993 provides a good framework. Moreover, S. 1993 contemplates that agencies will receive appropriate funding and personnel authority. IT security will not happen without appropriate funding and a core capability of skilled personnel. Nevertheless, there are current existing resources for effective controls ranging from guidance set forth in OMB Circular A-130[(3)] to the General Accounting Office's (GAO) various best practices guides, as well as the framework set forth in several recently enacted laws (e.g., Clinger-Cohen Act[(4)]). In addition, the Chief Information Officers (CIOs) individually and through their CIO Council have been studying and making recommen-dations in this arena. Also, various Inspectors General (IGs) have been active in providing recommendations through their reviews, audits and computer crimes investigations. One only needs to look through recent IG semiannual reports submitted to Congress to see the extensive activity by IGs in this arena. In the case of the NASA OIG, I refer you to our home page at http://oig.nasa.gov/ for the most recent semiannual report, as well as the full text of audits, reviews, and press releases of criminal investigations in the IT security arena.

DISCUSSION OF S. 1993

The proposed Act places responsibility on, accountability of, and coordination by some of the same players who made the Y2K readiness effort successful: OMB; the agency heads; the CIOs; GAO; and the IGs. In addition, because of the issues raised by information security, the Act also assigns specific roles to the Departments of Justice and Commerce, GSA, and law enforcement entities.

SUCCESS OF Y2K COORDINATED EFFORTS PROVIDES A MODEL FOR SIMILAR APPROACH TO IT SECURITY

It is worthwhile to briefly look at the mobilization of the Federal government in addressing the Y2K problem. That effort highlights what agencies can accomplish when there is sufficient priority placed on an initiative by the President, OMB, agency heads, the CIOs, GAO, IGs, as well as the Congress in the exercise of its oversight authority. The Y2K readiness effort forced the government into strategic management of its information resources.

Determined to avert potential catastrophic collapse of critical infrastructures, the Federal, state and local governments, as well as the private sector, attempted to identify the mission criticality of individual systems only to find such distinctions blurred by network interdependencies. End-to-end testing performed to assess Y2K readiness became a time-consuming enterprise in defining the boundaries of networked environments. As the new millennium approached, the Federal government focused increased attention on the problem. The President appointed a Special Assistant, John Koskinen, Chair of the President's Council on Year 2000 Conversion; the Congress initiated focussed oversight on agencies' readiness; OMB required department and agency heads to submit detailed reports; agency heads made clear the mandate to their staffs to place this effort as a high priority; and IGs and the GAO devoted substantial resources and efforts to help ensure that their agencies were going to be ready when the date changed. The focus worked: We entered the new millennium with minimal Y2K problems.

As discussed below, S. 1993 also assigns responsibilities to these same players (as well as additional entities) and gives each a responsibility for the success of information security.

ROLES SET FORTH IN S. 1993

OMB: The proposed bill gives wide latitude to OMB to take any authorized actions, including involving the budget or appropriations management process to enforce agency accountability for information resources. OMB will be required specifically to oversee and develop policies, principles, standards and guidelines for the handling of Federal information and information resources and to use its budgetary authority to enforce the accountability of the agency heads for information resources management and investments. Of course, OMB generally has these budgetary and policy authorities and has provided agencies considerable guidance (e.g., OMB Circular A-130). However, the explicit requirements emphasize the importance the Congress places on this effort. It re-emphasizes the mandate for OMB to hold agency heads accountable to implement information security and investment securities. Further, the Deputy Director for Management of OMB, to whom the Director may delegate the responsibilities under this proposed legislation, has a unique vantage point to coordinate efforts across the government by virtue of his/her role as Chair of the President's Management Council (PMC)[(5)]; the PCIE/ECIE; Chief Financial Officer[(6)] and CIO Councils initiatives. Planning responsibility at the Deputy Director level emphasizes to agency heads the importance placed on this initiative by the Congress.

Heads of Agencies: The agency heads occupy the "bully pulpit." They set the priorities of the Federal government by their personal involvement. It happened in the Y2K effort. It needs to happen in the IT security effort. This involvement means far more than issuing a memo or series of memos. The agency heads have to make clear that the current agency cultures, which permit very simple and avoidable vulnerabilities to occur and reoccur, are no longer acceptable.

Agency heads also have to ensure that their agency has sufficient trained personnel, a key requirement of the Act. Under the proposed Act, agency heads involvement extends to ensuring key officials (the CIO and senior program managers) perform their substantive responsibilities.

CIOs: The Act assigns considerable responsibility to CIOs for developing and maintaining agency information security programs, including assisting senior program managers in their responsibilities. The PCIE/ECIE working group noted that it would be helpful if the Act or legislative history provides greater guidance on the senior program manager function since that term is not defined in the proposed Act or existing legislation.

Some agencies might view the position as a very senior high level official; others, as the individual in charge of a specific program (e.g., Shuttle Program).

Requirements of the bill alone, however, will not ensure the CIOs' success. Most participants in the PCIE/ECIE working group felt that agency CIOs lacked the leverage and control of resources necessary to successfully develop, implement, and evaluate their agencies' information security programs. Some even expressed the opinion that their agencies' CIOs were, at best, "paper tigers." The proposed bill contemplates, and the group supports giving teeth to the position in order to ensure CIO responsibilities are effectively carried out. Congress will have to maintain oversight of the agencies' empowerment of their CIOs.

At NASA, the OIG has repeatedly recommended increased authority for the CIO. The Agency CIO has a limited staff and extremely limited budget (usually funds are provided for certain one time only NASA-wide purchases). The 10 Centers each have their own CIOs who collaborate with, but do not report to the NASA CIO. The Center CIOs each report to their Center's management who define their budgets, write their performance evaluations and allocate their staff positions. At some Centers, IT security resides in the security office; at other centers, it resides in the CIO's office.

In the past, we have been critical of this organizational approach to security by consensus because it results in delayed issuance and implementation of policies and procedures. Compounding this organizational structure, NASA has intentionally decentralized the CIO responsibility for IT security, designating different centers as the "Centers of Excellence" for specific functions: Ames Research Center (California) for IT security; Kennedy Space Center (Florida) for one component of Communications Security (COMSEC)[(7)] (Central Office of Records for the safeguard and control of COMSEC material[(8)]) with overall COMSEC management maintained within the Security Management Office at Headquarters; Goddard Space Flight Center (Maryland) for network incident response; Glenn Research Center (Ohio) for IT security training; and Marshall Space Flight Center (Alabama) for firewalls. We question the effectiveness of decentralizing and fragmenting these functions. Consider for example NASA's designation of Ames as the Center of Excellence for IT security. Ames personnel can and do conduct research into technology solutions for various IT vulnerabilities. Moreover, Ames coordinates with the Center CIOs, at a minimum, during weekly telecons and extensive exchange of email communications. These are all important practices. However, this assignment of responsibility to Ames reduces NASA's ability to efficiently and effectively utilize the enormous resources for IT security concentrated in the Washington, DC, metropolitan area. For example, the following offices are all located in Washington, DC, or its environs:

- NASA, the CIO, as well as the Security Office in charge of classified information policies and procedures
- NASA OIG Computer Crimes Division forensics and media analysis
- NASA IT Security Council - quarterly meetings occur at Headquarters where NASA-wide issues impacting the funding, staffing and other IT security issues are discussed (the Ames IT Security manager travels from Ames to attend this meeting or is connected by telecon)
- NASA's Automated Systems Incident Response Capability (NASIRC)
- National Security Counsel
- NIST
- Department of Defense Joint Task Force -- Computer Network Defense (JTF-CND)
- Department of Justice (DOJ) Computer Crimes and Intellectual Property Section (DOJ unit in charge of prosecuting network crimes)

- National Infrastructure Protection Center (NIPC)[(9)]

The NASA IT Security Manager could benefit by establishing close personal contacts with staff at the above listed agencies in order to stay current in their assessments of vulnerabilities, standards and best practices.[(10)] In the NASA OIG, we spend considerable time networking with these agencies to gain proficiency in IT security.

The proposed legislation requiring the CIO to designate a senior agency Information Security Officer will not address this decentralization at NASA. The Act does not require this position to report to the CIO, nor that this position be located in the CIO's office.

From our past work, we have seen very concrete examples where the decentralized structure weakened NASA's IT security posture. For example, NASA descoped the funding and responsibility NASIRC, a widely respected network incident response center, by fragmenting responsibility for its oversight at two centers, Ames (the Center of Excellence for IT security) and Goddard (the Center of Excellence for response). The Goddard Contracting Officer and Contracting Officer Technical Representative (COTR) performed oversight. Moreover, Centers differed widely in reporting intrusions to NASIRC. The absence of full reporting impacted the ability of the NASIRC to "connect the dots", to see the pattern of intrusions, and thereby, perhaps to discern the intent of the hackers and to prepare proper advice and warnings to the NASA Centers. The failure to report incidents also materially impacted on the ability of NASA OIG Computer Crimes Division (CCD) to be able to discern the pattern of criminal intent identify those conducting malicious attacks against NASA's systems. Because of these issues, my inspections unit conducted an assessment and made 11 recommendations to strengthen NASIRC. Management concurred, and we will conduct follow-up to ensure recommendations are fully implemented.

Inspectors General (IGs): S. 1993 provides for responsibility of the IGs appointed under the IG Act of 1978 (5 U.S.C. App.) to perform annual evaluations and tests of the agencies' compliance with the IT security requirements of the Act. Alternatively, an independent auditor, as determined by the IG of the agency, can perform the annual evaluation requirements.

The PCIE/ECIE working group recommended that the Act apply to all IGs. As written, Presidentially appointed IGs created after the original Act of 1978 (e.g., the IG at Department of Justice) would not be included, nor would any ECIE IGs. The proposed change would also ensure that the IG of the agency would be the selecting official for the independent evaluator in all instances, not the head of the agency. The working group also commented that the outside reviewer should not be narrowly defined as an "independent external auditor" (implying a financial orientation), but instead, be any qualified external entity.

The PCIE/ECIE working group discussed the issue of the resources required for performing the annual review. To place their comments in context, I think it is instructive for the Committee to understand the OIGs' experience with the Chief Financial Officer (CFO) audits. The financial audit reports were annual and could be performed by the OIG or by an independent external auditor. In order to meet their requirements under the CFO Act, the OIGs dedicated substantial staff and budget.

In NASA's case, the Agency and OMB supported staffing increases (approximately 10 additional auditors) during the period the OIG performed the audit. Both the Agency and OMB's funding support and the CFO's substantial engagement enabled NASA to be one of the first Federal agencies to receive an unqualified opinion. Once NASA received two

unqualified opinions from the NASA OIG, the Agency continued to support the CFO audit requirements by funding the external independent audit contract selected by the OIG. The OIG continued to dedicate staff to perform oversight of the contract, including the assurance that the independent audit met generally accepted government auditing standards.

Similarly, the annual report envisioned by the S. 1993 will require substantial personnel and budget commitment by each agencies' IG. In the case of the NASA OIG, information technology (IT) security has been one of the highest priorities of my office. The OIG currently has a robust program of criminal investigation, inspection, and audit activity focusing on protecting NASA's information resources and aggressively pursuing felonious intrusions resulting from hostile attacks on NASA information systems.

At the outset of my tenure, I was personally committed to building an IT audit, evaluation, and investigation IT security capability because of NASA's extensive dependence on network systems. In order to create the IT capabilities, I used vacancies created in other program areas. The Computer Crimes Division (CCD) is small, but smart and efficient.[(11)] Because I have recruited skilled staff for the computer crimes unit, they are usually at high grades; they are worth it.

The creation of the IT audit unit consisted of recruiting a handful of auditors and evaluators with some IT familiarity and training in-house auditors over the last four years. They began with very simple audits and received targeted training prior to each audit. They are now demonstrating increased skills, so they are able to perform more complex audits.

The office has made numerous recommendations to improve NASA's incident response capabilities and to protect sensitive technologies and other information from unauthorized access. For example, during an inspection, we uncovered security weaknesses involving data remaining on transferred and excessed personal computers.[(12)]

I have described the NASA OIG resource commitment so that the Committee will have a context to appreciate the comments on resources of the PCIE/ECIE working group. The reviews contemplated by S. 1993 will require recruiting, training and retaining a skilled set of personnel to perform the functions envisioned by the Act. The ability to perform the audits will be an evolving process. That also was the case for the CFO audits. Nevertheless, the investment in IT capability is well worth while for the oversight the IGs can provide and so should be supported by the agencies, OMB and the Congress through appropriate funding.

Law Enforcement Authorities: The Act provides that the CIO shall establish procedures for detecting, reporting, and responding to security incidents, including notifying and consulting with law enforcement officials and other offices and authorities. It also provides for notifying and consulting with an office designated by the Administrator of General Services within the General Services Administration.[(13)]

I want to address the CIO's requirements for "responding" and for "notifying law enforcement officials". The Act needs to make clear that the responsibility for "responding" to security incidents does not include "investigating" the incidents. Program officials by necessity have to perform some preliminary review in order to determine appropriate steps to protect critical systems and maintain operation and further analysis when they suspect potential crimes. However, systems administrators are not law enforcement investigators. The investigative role is reserved for special agents trained in

evidence collection, chain-of-custody issues, and other legal issues impacting admissibly of evidence and court presentations.

The Act is silent as to what entities are meant by "law enforcement officials". Where an OIG has established a computer crimes division,[(14)] then the agency system administrators need to report to the IG special agents. It is crucial for the system administrators to work in close cooperation with special agents who can suggest alternatives to preserving evidence while minimizing impact on operations.

Of course, OIG special agents are not the only law enforcement officials involved in investigations of cyber crime. Presidential Decision Directive (PDD) 63 addresses the protection of critical infrastructures that include physical and cyber-based systems essential to the minimum operations of the economy and the government. As part of the protection of the nation's critical infrastructure, PDD 63 establishes the National Infrastructure Protection Center (NIPC) to, among other duties, "… serve as a national **critical** (bold in the original) threat assessment, warning, vulnerability and law enforcement investigation and response entity". The NIPC's role for critical infrastructure protection only reinforces the key role of Inspectors General to conduct investigation of agency network crimes. OIGs, because of their audit, inspection and investigative activity, are able to make key linkages about criminal activity and the need for better internal controls in their agencies. The legislative history of the IG Act makes this linkage one of the key reasons for creating OIGs.[(15)]

> [The OIG] provides a single focal point in each major agency for the effort to deal with fraud, abuse and waste in federal expenditures and programs. Without that focal point, the linkage between auditing and investigating is likely to be ineffective. … Additionally this type of coordination and leadership strengthens cooperation between the agency and the Department of Justice in investigating and prosecuting fraud cases. The Department testified emphatically that those agencies which have been effective co-partners with the department have been those with viable offices of Inspector General.
>
> Senate report no. 95-1071, pp.2681-2682.

The Department of Justice has made clear that it does not contemplate that only the FBI has the authority to investigate or track computer offenses. Scott Charney, former Chief, Computer Crime and Intellectual Property Section, Department of Justice, wrote a letter dated February 1, 1997, to then Chair-Nominee of the President's Commission on Critical Infrastructure Protection. Mr. Charney stated:

> ... Second, I must correct the impression that at the federal level, only the FBI and the Department of Justice have the authority to investigate or track such attacks (computer offenses). Since 1984, when Congress passed the first computer crime statute, the U.S. Secret Service has had explicit jurisdiction over some kinds of computer crimes, along with the Federal Bureau of Investigation, which has general jurisdiction in this area. See 18 U.S.C., Sec 1030(d). In addition, many Federal agencies have criminal investigators with the training and the mission to investigate computer crimes directed against their own agencies. Some of these organizations, like the U.S. Air Force Office of Special Investigations, and the NASA Inspector General, have been leaders in this field.

As stated previously, IG special agents work closely with the Attorney General. The Department of Justice attorneys will function as the "honest broker", providing the proper coordination where IGs need to be working closely with the NIPC. The NIPC's focus is

critical infrastructure. But there are thousands and thousands of daily intrusions. The NIPC does not investigate all of the thousands of agency intrusions because they are not all against the critical infrastructure. OIG special agents are the chief investigators for their victim agencies. The Act or report language should emphasize the important role of IGs in protecting their victim agencies.

CONCLUSION

In summary, the Act importantly recognizes that IT security is one of the most important issues in shaping future Federal planning and investment. By highlighting OMB's role, the Act recognizes that IT planning does not stop at the doorstop of any agency. By focusing on the roles of the agency heads and CIOs, the Act makes it clear that each agency must be far more vigilant and involved than current practices.

The IG community has already been involved in IT security oversight and criminal investigation of network intrusions. S.1993 provides an even greater role. This task will require IG commitment of staff and other resources. The agencies, OMB and Congress need to provide the leadership and budgetary support for all the key players the Act enlists to defend the nation's network systems.

FOOTNOTES:

1. Executive Order No. 12805, Integrity and Efficiency in Federal Programs, May 11, 1992, established the PCIE and ECIE. These Councils are chaired by the Deputy Director for Management of the Office of Management and budget (OMB) and are comprised of Federal agency Inspectors General (IGs). IGs meet regularly to identify, review, and discuss areas of weakness and vulnerabilities to fraud, waste, and abuse in Federal programs.

2. On February 4, 1998, the President issued Executive Order 13073, "Year 2000 Conversion," stating that, because of a design feature in many electronic systems, some computer systems and other electronic devices may misinterpret the date change to the year 2000. This flaw was labeled the "Y2K problem" because it could cause systems to compute erroneously or simply not run.

3. OMB Circular A-130 calls for a plan for adequate security of each general support system and major application as part of the organization information resources management planning process. The security plan shall be consistent with guidance issued by the National Institute of Standards and Technology (NIST). Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. A summary of the security plans shall be incorporated into the strategic information resources management plan required by the Paperwork Reduction Act (44 U.S.C. Chapter 35) and Section 9(b) of the circular.

4. The Clinger-Cohen Act of 1996 has established within Federal agencies the corporate framework for management of information resources, including both government information and information technology. The establishment of Chief of Information Officers was singularly one of the most positive steps taken to focus attention on the management of information. Importantly, the Act called for a comprehensive information technology architecture that provides the integrated framework for both existing and newly acquired hardware and software.

5. President's memorandum, October 1, 1993, reprinted at 58 FR 52393, established the President's Management Council (PMC). The PMC consists of the Chief Operating Officers of all Federal departments and the largest agencies. The PMC provides leadership for the most important Government-wide reforms.

6. Pursuant to 31 USC, Section 90, Chief Financial Officers are appointed or designated for major Federal agencies and are responsible for agency policies, guidelines, and procedures for budget and financial management functions.

7. COMSEC generally encompasses secure measures and controls taken to deny unauthorized persons information derived from telecommunications and ensures the authenticity of such telecommunications. Communications security includes crypto-security, transmission security, emission security, and physical security of COMSEC material. For example, COMSEC measures are applied to protect the command and control communication links with the Space Shuttle.

8. COMSEC Central Office of Records (COR): the NASA COR provides centralized management and control of all COMSEC material held by NASA COMSEC accounts. NASA COR responsibilities include: establishing and closing COMSEC accounts; and establishing or approving accounting procedures for accounts under its cognizance.

9. See page 15-17 for a discussion of the NIPC's role in IT security.

10. Moreover, it's been our experience that it is extremely difficult for Government to recruit and retain highly skilled computer professionals in the Ames area due to its high cost of living and proximity to California's Silicon Valley (San Jose).

11. As part of their efficiency and economy, the CCD forms partnerships for tool development and share resources with entities such as the Department of Defense Computer Forensics Laboratory (DCFL). DCFL's mission includes providing digital evidence processing, analysis and diagnostics for DoD criminal, fraud, and counterintelligence investigations, operations and programs. We hope to continue forming partnerships with others in such areas as training.

12. My office has published an instructional brochure on properly clearing data from hard drives, which I have previously provided for your information and use. This pamphlet was widely distributed throughout NASA and the IG community.

13. The PCIE/ECIE working group could not comment about the GSA provisions because we were unsure which offices set forth in S. 1993 would perform the functions and responsibilities.

14. Not surprisingly, more Inspectors General are establishing computer crime units as their agencies are more and more turning to e-commerce to conduct business, solicit grants and contracts and to purchase supplies. Investigators will no longer be able to rely on the "paper trail" to identify their suspect. They must be able to retrieve evidence stored in a computer and know how to properly seize a computer used in the commission of crimes.

15. The IG Act specifically provides that the Offices of Inspector General were created to conduct and supervise investigations relating to the (Agency) programs and operations ..." of the Agency (Sec. 2).; "... to conduct, supervise, and coordinate audits and investigations relating to the programs and operations ..." of the Agency (Sec. 4(a)(1)); and in carrying out the duties and responsibilities established under this Act, each

Inspector General shall report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal ciminal law" (Sec. 4(d)).