Inspector General Reviews of Presidential Decision Directive 63 Implementation

Statement of

ROBERTA L. GROSS
Inspector General

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

Before the

Senate Committee on Governmental Affairs

Hearing on "How Safe Is Our Critical Infrastructure?"

September 12, 2001

I. INTRODUCTION

As a nation, we have become more aware about the vulnerability of critical infrastructures, particularly to cyber attacks.[1] Just consider recent NewsBites published by the SANS (Security Administration, Networking and Security) Institute.[2]

- August 30, Invalid Worm: "The "Invalid" Worm arrives as an attachment purporting to be a patch from Microsoft." The worm mass mails itself to users and, once launched from an attachment, encrypts executable files rendering them unusable.

- August 31, Two Arrested in Encryption Device Export Plot: "A four month long investigation led to the arrest of two men who allegedly tried to smuggle

[1]Events such as the bombing of the Murrah Federal Building in Oklahoma City demonstrated that the Federal government needed to address new types of threats and vulnerabilities, many of which had not previously received a high priority. The Executive Branch formed a critical infrastructure working group, which included representatives from the defense, intelligence, law enforcement and national security communities. The working group identified both physical and cyber threats as growing concerns. For purposes of my testimony, I am focusing on the cyber critical infrastructure.

[2]SANS is a cooperative research and education organization founded in 1989 through which systems administrators, security professionals and network administrators share information and lessons learned.

encryption devices to China. The devices in question are designed for government use."

- August 31, British Business Group Wants Government Help With Cybercrime: "The UK's Confederation of British Industry (CBI) wants the government to take action against cybercrime by establishing a center for incident reporting and by updating the 1990 Computer Misuses Act to include attacks on computer systems. CBI says that the fear of financial losses due to cybercrime is preventing e-commerce from blossoming."

- August 29, Bank Replacing Compromised Debit Cards: "Three thousand Riggs Bank Customers will receive new Visa debit cards after an apparent breach of security on a server that processes Visa transactions. While no resulting instances of credit(sic) card fraud have been reported, the bank did not want to take any chances."

Investigations by the NASA Office of Inspector General (OIG) Computer Crimes Division (CCD) result in similar articles and headlines. For example, a joint investigation by NASA OIG computer crime sleuths, the Department of Defense Criminal Investigation Service, and the Federal Bureau of Investigation (FBI) resulted in a 16 year old juvenile from Miami, FL, being sentenced to 6 months in a detention facility. (This was the first time a juvenile computer hacker was sentenced to serve time.) The individual admitted to illegally accessing 143 computers at the Marshall Space Flight Center, Huntsville, Alabama. He obtained and downloaded proprietary software from NASA valued at approximately $1.7 million. The software supported the International Space Station's physical environments, including control of the temperature and humidity of the living space. The juvenile's actions required that the systems be shut down, which caused delivery delays of the program software. This resulted in additional costs of $41,000 in labor and equipment replacement. He also had illegally accessed Department of Defense computer networks and obtained more than 3,300 electronic messages and 19 user names and passwords. His intrusion specifically targeted a U. S. Army procurement system computer and copied and transferred a highly sensitive password file. This activity caused a costly computer shutdown and subsequent maintenance and restoration costs.

Clearly, juvenile hacker activity can be more than a mere nuisance!

In another recent investigation by the OIG CCD, a former NASA contractor employee and two others were sentenced for using NASA computer equipment to develop programs that allowed them to illegally capture ATM accounts and

Personal Identification Number (PIN) numbers to steal large sums of money from unsuspecting bank customers.

The harm caused by hackers is compounded because many hackers share their access with countless others by publicizing their exploits, tools and stolen passwords on Internet chat rooms. For example, OIG CCD agents, together with local law enforcement officials, arrested a hacker who illegally accessed a NASA computer system at one of NASA's research centers, obtained passwords and posted this information on the Internet.

The threats are also from international sources. Consider the following investigations conducted in parallel by the NASA OIG CCD and the FBI. In March 1998, CCD agents arrested one of the U. S. ringleaders of the Internet hacking group known as "ViRii". Our investigation revealed evidence about "ViRii" breaking into a large number of government, corporate, and university Internet-based systems. The NASA investigation into "ViRii" began in June 1997, when it became known that a NASA Jet Propulsion Laboratory (JPL) (Pasadena, CA) server was controlled and used by a number of U. S. and foreign hackers. The OIG CCD investigation identified the "ViRii" ringleader and others as possible suspects, including an Israeli national known as "Analyzer". In February 1998, separate attacks against other U. S. government sites caused the FBI and the Air Force Office of Special Investigations (AFOSI) to focus on "Analyzer". The FBI executed search warrants against two juveniles on February 25, 1998, in Cloverdale, California, to recover evidence of "Analyzer" related intrusions.

"Analyzer" is an Israeli citizen who was subsequently arrested in Israel based on evidence provided to Israeli authorities by a delegation of U. S. Federal Agents from Air Force Office of Special Investigations, FBI and the NASA CCD. The "ViRii" leader, the juvenile, and the Israeli all have been sentenced and/or adjudicated for their activities.

These examples demonstrate that network interconnectivity, while increasing productivity, clearly creates serious vulnerabilities.[3] The threats from the network even reach into our personal lives. The Internet exposes our very identities to theft when hackers steal vital information, including social security numbers, credit card numbers, etc. The NASA OIG has published a guide on preventing identity theft through computers in a brochure, "Protect Yourself and NASA Before Getting Rid of That Old Home Computer"

[3]Hackers can be insiders who are motivated by revenge, financial gain, and/or stress. External perpetrators are diverse, including teenagers showing off their skills; electronic protestors; terrorists; or possibly even foreign intelligence services.

(http://www.hq.nasa.gov/office/oig/hq/identify/html). Even simple acts of charity performed individually or as a government can be harmful (e.g., donating excess computers to organizations such as schools and prisons. Failure to properly and completely clear hard drives may expose confidential, sensitive, or proprietary information to unauthorized persons. The NASA OIG has issued several reports to NASA on this topic following inspections of excessed or surplused hard drives containing sensitive information. We also published a brochure widely distributed to the Agency, the IG community, and to Congress on the risks of carelessly excessing computers without sufficiently clearing hard drives. This brochure, "Clearing Information From Your Computer's hard Drive," is available at http://www.hq.nasa.gov/office/oig/hq/harddrive.pdf.

II. PDD 63: ROLE OF INSPECTORS GENERAL[4]

The current Administration views securing the nation's critical infrastructure as a priority. The previous Administration established this priority through the issuance of Presidential Decision Directive 63 (PDD 63) on May 22, 1998. PDD 63 sets forth the mandate to protect our Nation's critical infrastructures[5] from acts that would significantly diminish the abilities of:

---

[4]Today's civilian Inspectors General (IGs), created by the Inspector General Act of 1978, as amended, independently review the programs and operations of their agencies; detect and prevent crime, fraud, waste, and abuse; and promote economy, efficiency and effectiveness so that their agencies can effectively serve the public. In simple terms, the IGs have three basic roles: to foster good program management, to prevent future problems, and deter, abate and punish crime and fraud.

IGs report both to the head of their respective agencies and to the Congress. This dual reporting responsibility is the framework within which IGs perform their functions. Unique in government, it is the legislative safety net that protects the IGs' independence and objectivity.

Collectively, during FY 2000, the IGs were responsible for:

- Potential savings of $9.5 billion.
- Recovery actions of almost $5.5 billion.
- More than 5,500 successful prosecutions.
- Suspensions or debarments of nearly 7,000 individuals or businesses.
- More than 2,600 civil or personnel actions.
- More than 120 testimonies before the Congress.

[5]PDD 63 defines critical infrastructures as "those physical and cyber-based systems essential to the minimum operations of the economy and government. . . . Many of the Nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked."

- the Federal government to perform essential national security missions and to ensure the general public health and safety;

- state and local governments to maintain order and to deliver minimum essential services; and

- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial, and transportation services.

PDD 63 assigns responsibilities to various groups, agencies and offices to achieve the protection of the Nation's critical infrastructure. Because of the importance of implementing this initiative, 21 agency and departmental (hereinafter agency) IGs agreed to review the progress by their agencies in carrying out their responsibilities to protect the nation's and their agencies' critical infrastructures. My office is coordinating this effort on behalf of the President's Council on Integrity and Efficiency (PCIE) and the Executive Council on Integrity and Efficiency (ECIE).[6]

As an aside, it is fitting that IGs are reviewing their agencies' infrastructure protection readiness. Since the Revolutionary War, military IGs have been tasked with independently reviewing the combat readiness of American troops. Today, the readiness needs of this nation call for different rules of engagement and the tools of future conflicts will be more diverse. PDD 63 was promulgated

---

[6]The IGs coordinate their professional activities through the PCIE and ECIE, which were established by Executive Order 12805. These councils work to promote collaboration on integrity, economy, and efficiency issues that transcend individual governmental agencies and to increase the professionalism and effectiveness of OIG personnel throughout the Government.

The PCIE is primarily comprised of the Presidentially appointed IGs and the ECIE is primarily comprised of IGs chosen and approved by heads of their agencies. The Deputy Director for Management of the Office of Management and Budget (OMB) chairs both Councils. Officials from the Federal Bureau of Investigation, Office of Government Ethics, Office of Special Counsel, and Office of Personnel Management serve on both Councils.

Recent projects by the Councils include:

- A Government-wide audit of non-tax delinquent debt ($46.4 billion at the time of the audit), which made a number of recommendations to enhance Federal debt collection.
- Special editions of *The Journal of Public Inquiry*, including a January 2001 issue to alert the new Administration to the key management challenges they would be facing.
- A Government-wide project to ensure Federal employee compliance with child support enforcement.
- Workshops on the implementation of the Government Information Security Reform (GISR), Title X, Subtitle G, of the 2001 Defense Authorization Act, approved October 30, 2000. See note 4, below.

as a step in implementing an adequate defense system for future potential conflicts.

The IGs are performing this important role in the infrastructure protection of the United States by establishing a Government-wide approach for assessing each agency's readiness for this critical challenge. The approach consists of four phases. Phase I relates to the adequacy of agency planning and assessment activities for protecting cyber-based infrastructures. Phase I has been completed and will be discussed below. Phase II, the review of the implementation of cyber plans, has been deferred to allow the agencies time to develop, implement, and evaluate their plans. Phase III, now in progress, will monitor agencies' planning and assessment activities related to critical physical structures. Phase IV will review the implementation of the plans related to the critical physical structures. We anticipate the completion of Phase III and the initiation of Phase II will occur sometime this Fall after the IGs forward their GISR reports related to their agencies' information security. The GISR effort complements PDD 63 activities.[7]

PDD 63 PHASE I REVIEW RESULTS:

On March 21, 2001, the PCIE/ECIE issued a report to the Honorable Mitchell E. Daniels, Jr., Director, Office of Management and Budget and Mr. Richard Clarke, National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism, National Security Council, reflecting generally the Phase I findings of the 21 participating OIGs. Our reviews summarized below demonstrated collectively that the Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. It is, however, important to view these criticisms in the proper context; that is, because of the focus on critical infrastructure required by PDD 63, the nation is already in a better position because it is starting down the path towards a more robust effort to protect the Nation's critical infrastructure.

I will briefly highlight our collective findings in five areas:

- Misunderstanding of the applicability of PDD 63
- Imprecise performance measures
- Untimely identification of critical infrastructures

[7]GISR primarily addresses the program management, implementation and evaluation of security related both to unclassified and national security systems. The Act directs IGs or their designees to perform annual independent evaluations of their respective agencies' information security programs and practices. The agencies, likewise, are required to submit an annual evaluation report to Congress. On September 10, 2001, each agency submitted a combined agency and IG report to OMB, summarizing IT security and related issues.

- Lack of coordinated management of PDD 63 requirements
- Failure to advance beyond the planning stage

Applicability of PDD 63

Not all agencies began to implement PDD 63. Several agencies mistakenly believed that PDD 63 only applied to the specific agencies listed in the Directive and its addendum.[8] This misimpression was reinforced by an inaccurate interpretation by a key Federal player in overseeing the implementation of PDD 63. However, PDD 63 clearly applied to all agencies. PDD 63 Section VII, Protecting Federal Government Critical Infrastructures, provides,

> Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of the other aspects of that department's critical infrastructure. (Emphasis supplied.)

As a result of the misinterpretation, certain agencies did not prepare the required critical infrastructure plans and did not identify minimum essential infrastructures (MEIs). MEIs are defined as "the framework of critical organizations, personnel, systems and facilities that are absolutely required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services". Almost none of the agencies had performed vulnerability assessments of their MEI assets or developed remediation plans.

Most of the agencies that did not know PDD 63 applied to them began to address the Directive requirements as a result of the IG reviews.

Performance Measures

---

[8]PDD 63 identified only certain agencies for specific tasks: Commerce – information and communications; Treasury – banking and finance; EPA – water supply; Transportation – aviation, highways (including trucking and intelligent transportation systems), mass transit, pipelines, rail; waterborne commerce; Justice/FBI – emergency law enforcement services; FEMA – emergency fire service, continuity of government services; HHS – public health services, including prevention, surveillance, laboratory services, and personal health services; Energy – electric power, oil and gas production and storage; Lead Agencies for Special Functions: Justice/FBI – law enforcement and internal security; CIA – foreign intelligence; State – foreign affairs.

Agencies were told they were required to achieve a level of security preparedness, or "Initial Operating Capability" (IOC), no later than December 31, 2000. However, agencies were not provided a uniform definition of IOC and so there was no consistent implementation. For example, one agency defined IOC to mean "completion of those initial mediation measures that are identified as needed by that time during the vulnerability assessment/mitigation planning process." Representatives responsible for implementing PDD 63 in that agency said they could not understand the agency's definition of IOC. Another agency gave an entirely different definition of IOC: "(1) a broad level assessment of MEIs should be completed, (2) remediation plans should be completed for assets considered to be the most at risk, and (3) fixes should be in place for the most vulnerable assets." Without an adequate and consistent definition, the Federal Government can not adequately measure progress towards achieving full security preparedness.

Identification of Critical Infrastructure

At the time of the reviews, for a variety of reasons, most of the agencies which had submitted Critical Infrastructure Plans (CIPs)[9] had not identified and/or adequately identified their critical, cyber infrastructure assets. The reasons included lack of funds, poor methodology for identifying assets, and "higher priority" work.

The Executive Branch announced a standardized but non-mandatory process for identifying critical infrastructure assets entitled "Practices for Security Critical Information Assets." It also initiated Project Matrix, an ongoing effort that utilizes a multi-agency team evaluation to apply the Practices. Project Matrix involves a three-step process. In Step 1, the Project Matrix team identifies and prioritizes each agency's PDD 63-relevant assets. In Step 2, the the major nodes and networks upon which the most critical assets depend and identifies significant points of failure. In Step 3, the team identifies the infrastructure dependencies associated with select assets identified in Step 1 and analyzed in-depth in Step 2. The project Matrix guidance and process were not mandatory and generally had to be funded by the subject agency. Its success was limited by the amount of time and funds available to implement the process.

Management of PDD 63 Activities

[9]PDD 63 requires that not later than 180 days from its issuance, every agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems.

The Federal organizations primarily responsible for implementing PDD 63 did not coordinate and manage their PDD 63 activities. The following organizations are among those responsible for coordinating and/or managing PDD 63 implementation:

- The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism is responsible for coordinating and implementing the Directive. The National Coordinator cannot direct departments and agencies but will ensure interagency coordination for policy development and implementation.
- The Office of Management and Budget is responsible for developing information security policies and overseeing agency practices.
- The National Institute of Standards and Technology is responsible for developing technical standards and providing related guidance for sensitive data.
- The National Security Agency is responsible for setting information security standards for national security agencies.
- The National CIAO, an interagency office, is responsible for developing an integrated National Infrastructure Assurance Plan to address threats to the Nation's critical infrastructure.
- The General Services Administration is the designated lead agency for the Federal sector.

The absence of coordinated oversight and management of PDD 63 has caused certain fundamental elements of the Directive to receive less than adequate attention.[10] As discussed earlier, several agencies had mistakenly decided not to implement PDD 63 because they believed, based in part on guidance from a key player in PDD 63 implementation, that they were exempt from the Directive.

Advancing Beyond the Planning Phase

---

[10]In April 2001, the U. S. General Accounting Office (GAO) submitted a report to the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U. S. Senate, "Critical Infrastructure Protection: Significant Challenges Developing National Capabilities (GAO-01-323). This report focused on the progress on the FBI's National Infrastructure Protection Center (NIPC) which, under PDD 63, had the role of providing comprehensive analyses on threats, vulnerabilities, and attacks; issuing timely warnings; facilitating and coordinating the law enforcement investigation on critical cyber infrastructure attacks. The GAO report noted the need for improvement in establishing information sharing partnerships between the NIPC and the private sector and other Federal Government agencies. The PCIE/ECIE group has not evaluated the NIPC's relationships with their agencies or the IG law enforcement community.

Some agencies have not performed vulnerability assessments of their critical infrastructure assets or prepared the related remediation plans. This condition occurred because the budget requests that the agencies submitted to the OMB were rejected by OMB as not sufficiently detailed to justify funding the agencies' Critical Infrastructure Plans (CIPs) requirements.

The National Plan for Information Systems Protection, Version 1.0, "An Invitation to a Dialogue," acknowledged that the quality of the agencies' CIP budget requests did not meet OMB's expectations:

> Agency budget systems don't readily support collection of CIP data. Until these systems are modified, collection of information on CIP programs and budgets will be manual and inexact. The newness of CIP also means that the government is still on the steep part of a precipitous learning curve. Individual agencies are still grappling with the issue internally and the interagency process is still coming together. . . . When OMB issued its first CIP Budget Data Request (BDR) last year, it sought information at an activity level. But because of inadequate activity descriptions and data presentation problems, it was unable to consolidate the data, making it difficult to identify programmatic duplications and gaps that point up inconsistencies needing analysis and remedy. All this reduced confidence in the data.

III. NEXT STEPS

We made general suggestions to OMB based on our findings. Generally, these suggestions related to the need to better define terms, measures, and expectations set forth in PDD 63. Our suggestions also covered the need to ensure better coordination among the entities and organizations responsible for PDD 63 implementation.

We understand that in the very near future the White House will be issuing further guidance on protection of the nation's critical infrastructure. The PCIE/ECIE effort (coordinated by the NASA OIG) will play a part in this national effort by continuing the Government-wide review. This review will provide important feedback to heads of departments, OMB, other Executive entities, and the Congress. Also, individual IGs will have a vital role to play in the detection, deterrence, and prosecution of those committing cyber crimes against their victim agencies. With the Federal Government expanding e-government and e-commerce, the IGs necessarily will increase their criminal investigations in the cyberworld.

IV. CONCLUSION

PDD 63 provides an important focus on the Nation's critical infrastructure. The PCIE/ECIE found mixed progress in the Federal Government's implementation of this Directive. However, important steps have been taken. These steps must continue to ensure that our Nation has the capability to meet the growing threat of physical and computer-based attacks that potentially could cripple, disrupt and/or damage our critical infrastructure.

IGs have a unique role in assisting their agencies' critical infrastructure and planning implementation because of their ability to coordinate audits, inspections, and criminal investigation resources. They also will individually and collectively play a key role in the Nation's infrastructure protection through their reviews and cybercrime investigations.