PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY

March 21, 2001

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
Old Executive Office Building
Washington, D.C. 20503

Dear Mr. Daniels:

The President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) recently completed Phase I of a four-phase review of Federal agencies' implementation of Presidential Decision Directive (PDD) 63. PDD 63 calls for assuring the security of the nation's critical infrastructures. Under this Directive, the United States is expected to take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on the nation's critical infrastructures.

Our overall objective was to review the adequacy of the Federal Government's critical infrastructure protection program relative to the PDD 63 requirements. In Phase I, we reviewed the planning and assessment activities for cyber-based infrastructures. The National Aeronautics and Space Administration (NASA), Office of Inspector General (OIG), led the review of 21 participating OIGs. All participants either have or will be issuing individual reports to their respective departments or agencies.

In short, the Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. The OIG reports issued to date present findings that, collectively, question the government's ability to achieve the required full operating capability by May 22, 2003. Key factors impacting the implementation of PDD 63 are listed below and discussed in more detail in the attached report:

- Misunderstanding as to the applicability of PDD 63.
- Imprecise performance measures.
- Untimely identification of critical infrastructures.
- Lack of coordinated management of PDD 63 requirements.
- Failure to advance beyond the planning phase.

We appreciate your consideration of these matters. If you have any questions or comments, please call Russell A. Rau, NASA Assistant Inspector General for Auditing, at (202) 358-4458.

Sincerely,

Gaston L. Gianni, Jr.
PCIE Vice Chair

Barry R. Snyder
ECIE Vice Chair

PRESIDENT'S COUNCIL on INTEGRITY & EFFICIENCY
EXECUTIVE COUNCIL on INTEGRITY & EFFICIENCY

March 21, 2001

The Honorable Mitchell E. Daniels, Jr.
Director
Office of Management and Budget
Old Executive Office Building
Washington, D.C. 20503

Dear Mr. Daniels:

This letter presents the Phase I results of a four-phase President's Council on Integrity and Efficiency (PCIE) and Executive Council on Integrity and Efficiency (ECIE) review of Federal agencies' implementation of Presidential Decision Directive (PDD) 63 related to critical infrastructure protection. The National Aeronautics and Space Administration (NASA), Office of Inspector General (OIG), led the review that included participation of a total of 21 OIGs. All participants either have or will be issuing individual reports to their respective departments or agencies.[1]

Based on the Phase I review results, we are providing our observations and suggestions for strengthening the Federal Government's compliance with PDD 63. The review identified several key areas where improvements can enhance the security of our nation's critical infrastructures.

Background

When signed on May 22, 1998, PDD 63 called for a national effort to assure the security of the nation's critical infrastructures.[2] Under the Directive, the President intends that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on the nation's critical infrastructures, especially its cyber systems. By May 22, 2003, the United States shall have achieved and shall maintain the ability to protect its critical infrastructures from intentional acts that would significantly diminish the abilities of:

- 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 public services; and

[1] Departments and agencies are hereafter referred to as agencies.
[2] PDD 63 defines critical infrastructure as " . . . those physical and cyber-based systems essential to the minimum operations of the economy and government." Critical infrastructures include, but are not limited to, telecommunications, banking and finance, energy, transportation, and essential government services.

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

Various laws and regulations have addressed the need to secure our nation's key cyber systems including the Government Information Security Reform Act; the Clinger-Cohen Act; the Computer Security Act; and Appendix III to Office of Management and Budget (OMB) Circular A-130, "Security of Federal Automated Information Resources." PDD 63 complements and expands on those laws and regulations by requiring an independent review of security plans for protecting the nation's critical systems; the identification of minimum essential infrastructure (MEI)[3] critical to the operations of the economy and government, including infrastructure interdependencies; and the assessment of MEI vulnerabilities.

On November 17, 1999, the PCIE and ECIE formed a working group to review the Federal agencies' implementation of PDD 63.

Objectives, Scope, and Methodology

Our overall objective was to review the adequacy of the Federal Government's critical infrastructure protection (CIP) program in the context of PDD 63 requirements. The review consists of four phases. Phase I relates to planning and assessment activities for cyber-based infrastructures; Phase II, implementation activities for cyber-based infrastructures; Phase III, planning and assessment activities for physical minimum essential infrastructures; and Phase IV, implementation activities for the physical minimum essential infrastructures. Participating OIGs were responsible for (1) determining the scope of their reviews, (2) performing review work at their respective agencies, and (3) providing the PCIE/ECIE Working Group with a summary of their review results. Also, the Working Group reviewed the coordination activities of the Federal organizations primarily responsible for implementing PDD 63. The 21 OIGs that participated in the Phase I Review are listed in the Enclosure.

In Phase I, the participating OIGs reviewed the adequacy of agency cyber-based plans, asset identification efforts, and initial vulnerability assessments. Specifically, the OIGs determined whether agencies had:

- developed effective plans for protecting their critical cyber-based infrastructures;
- identified their cyber-based MEI and interdependencies; and
- identified the threats, vulnerabilities, and potential magnitude of harm to their cyber-based MEI that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of their critical cyber-based infrastructure investments, and developed remediation plans to address the risks identified.

[3] The Critical Infrastructure Assurance Office (CIAO) has defined agency MEI 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."

Overall Review Results

The Federal Government can improve its PDD 63 planning and assessment activities for cyber-based critical infrastructures. Specifically, the review determined that:

- Many agency infrastructure plans were incomplete.
- Most agencies had not identified their mission-essential infrastructure assets.
- Almost none of the agencies had completed vulnerability assessments of their MEI assets or developed remediation plans.

When all participating OIGs complete their Phase I Reviews, they will have made an estimated 100 recommendations to improve their respective agency's CIP program.

The OIG reports issued to date present findings that, collectively, question the Federal Government's ability to achieve full operating capability by May 22, 2003, as required by PDD 63. Key factors impacting the agencies' ability to implement PDD 63 are:

- Misunderstanding as to the applicability of PDD 63.
- Imprecise performance measures.
- Untimely identification of critical infrastructures.
- Lack of coordinated management of PDD 63 requirements
- Failure to advance beyond the planning phase.

Each of these factors is discussed below.

Applicability of PDD 63

Several agencies decided to not implement PDD 63 because they believed they were exempt from the Directive. They based their decision on the mistaken belief that PDD 63 applied only to the 19 agencies listed in the Directive and its addendum. As a result, agencies considering themselves exempt from PDD 63 had not prepared the required CIP plans, identified their MEI assets, performed vulnerability assessments of their MEI assets, or developed remediation plans. Most of them have now initiated work to address PDD 63 requirements as a result of our review.

The Director, National Critical Infrastructure Assurance Office (CIAO),[4] told PCIE/ECIE Working Group members that all agencies are subject to PDD 63. The Director highlighted two key criteria in PDD 63 to support his position.

[4] The National Critical Infrastructure Assurance Office supports the National Coordinator for Security, Infrastructure Protection, and Counter-Terrorism in developing an integrated national infrastructure assurance plan to address threats to the nation's critical infrastructures. The CIAO also coordinates a national education and awareness program, as well as legislative and public affairs initiatives.

> Section VII: 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 shall appoint a Chief Infrastructure Assurance Officer . . . who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure.
>
> Section V: The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.

Much of the confusion regarding the applicability of PDD 63 can be attributed to the Federal Sector Liaison[5] for PDD 63 who told representatives of the agencies not listed in the Directive, that nonlisted agencies were exempt from PDD 63 because they were not specifically identified in the Directive.[6]

We suggest that the Director, Office of Management and Budget, and the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council, direct the National CIAO to advise all Federal agencies of their responsibilities for implementing PDD 63.

Performance Measures

Agencies were required to achieve a level of security preparedness (referred to as initial operating capability (IOC)), not later than December 31, 2000, but had not been advised of the requirements for achieving IOC. Neither the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism (who authored the term) nor the Director, National CIAO, had defined IOC. Without a formal definition, achievement of IOC is not a consistent measure of progress toward achieving full security preparedness.

Because the term IOC has not been defined, agencies have used various interpretations. 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 defined IOC as: "(1) a broad level assessment of MEI 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."

Although the date for achieving IOC has passed, agencies still need guidance for measuring their progress in completing the identification of critical infrastructure assets, performing vulnerability assessments, developing remediation plans, and implementing the remediation plans. Until such guidance is established, the government continues to lack the visibility needed to accurately assess the status of its infrastructure protection program.

---

[5] The Federal Sector Liaison is located at the General Services Administration.
[6] The Federal Sector Liaison confirmed his interpretation of the scope of PDD 63 to the NASA OIG.

We suggest that the Director, Office of Management and Budget, and the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, National Security Council, provide guidance that agencies can use to measure their progress in achieving full operating capability.

Identification of Critical Infrastructure

Most of the agencies having CIP plans had not identified or adequately identified their critical, cyber infrastructure assets.[7] The National CIAO has established an asset identification initiative (Project Matrix, discussed below) that agencies can use to identify their critical assets. Unfortunately, the initiative may end before most agencies have had an opportunity to participate in it. Without an accurate and complete inventory of critical assets, agencies cannot identify and remediate their security-related vulnerabilities.

In a July 19, 2000, memorandum, the National Coordinator announced a standardized process, to be administered by the National CIAO, for identifying critical infrastructure assets initially at 14 agencies. The process, called Project Matrix, would:

> . . . identify all assets, nodes and networks, and associated infrastructure dependencies and interdependencies required for the Federal Government to fulfill its national security, economic stability, and critical public health and safety responsibilities to the American people. In this context, the word "critical" refers to those responsibilities, assets, nodes and networks that if incapacitated or destroyed would: jeopardize the nation's survival; have a serious, deleterious effect on the nation at large; adversely affect large portions of the American populace, and require near-term, if not immediate, remediation.

The Project Matrix team is composed of employees from various agencies and disciplines whose goal is to apply a standard methodology and criteria for helping agencies identify their critical assets.

Although Project Matrix provides a rational and consistent approach for identifying critical infrastructure assets, its success will be diminished by the amount of time needed to implement the process and by the National CIAO's limited time left as a functioning office. Specifically, the Project Manager for Project Matrix stated that the Project Matrix team can review only six to eight agencies a year. In view of the much larger number of agencies that may have critical infrastructure assets, several years would be needed to review all assets. Further, Congress has authorized the National CIAO to function only through September 30, 2001. Without continued funding of the National CIAO, the future of Project Matrix is questionable.

We suggest that the Director, Office of Management and Budget, continue a matrix-like approach for the identification of critical infrastructures for all agencies that may possess them.

[7] This condition occurred for a variety of reasons including the lack of funds, poor methodology for identifying assets, and higher priority work.

Management of PDD Activities

The organizations primarily responsible for implementing PDD 63 have not effectively coordinated and managed their PDD 63 activities. This condition occurred largely due to the decentralized oversight and responsibilities of the entities implementing PDD 63. As a result, the Federal Government's ability to achieve full operational capability by May 2003, as required by PDD 63, is questionable.

The following organizations are among those responsible for coordinating and/or managing implementation of PDD 63:

- 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 infrastructures.
- The General Services Administration (GSA) 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. As discussed earlier, several agencies had mistakenly decided to not implement PDD 63 because they believed they were exempt from the Directive and have not established performance measures. Additionally, most agencies will not have benefited from Project Matrix by the time the program could cease to exist. Further, we found that the GSA's Federal Sector Liaison has provided limited direction or assistance to the agencies. Finally, the CIAO's Expert Review Team (ERT), which has reviewed and furnished comments to 22 agencies regarding their CIP plans, is no longer functioning.[8]

[8]The Department of Commerce fiscal year 2001 budget request states that the National Institute of Standards and Technology (NIST) will establish a permanent ERT to replace the interim ERT at the National CIAO. In December 2000, NIST authorized the establishment of a Computer Security Expert Assist Team to review agency security practices, policies, and procedures. As of March 12, 2001, NIST had not activated the Computer Security Expert Assist Team due to a Federal hiring freeze.

We suggest that the Director, Office of Management and Budget, assign one organization the appropriate leadership responsibility and authority for overseeing the implementation of PDD 63 and for achieving government-wide, full operational capability by May 2003.

Advancing Beyond the Planning Phase

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 not sufficiently detailed for OMB to consider in funding the agencies' CIP requirements. The agencies' ability to prepare detailed requests, however, requires that the agencies perform vulnerability assessments and develop remediation plans, an undertaking for which the agencies have lacked funding or have been unwilling to fund from other parts of their approved budgets. Accordingly, some agencies have not advanced their CIP programs beyond the planning phase almost 3 years after President Clinton signed PDD 63.

The National Plan for Information Systems Protection, Version 1.0, "An Invitation to a Dialogue,"[9] states that the quality of the agencies' CIP budget requests did not meet OMB's expectations for the following reasons.

> 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.

On March 8, 2000, OMB informed agencies that "extremely detailed" information regarding needed corrective actions must accompany the budget data submitted to OMB. This request also appears in OMB's Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," dated February 28, 2000, to remind agencies of OMB criteria for incorporating and funding security as part of the agencies' information technology systems and architectures and of the decision criteria that OMB will use to evaluate security for information systems investments. OMB issued the memorandum pursuant to the Clinger-Cohen Act, which directs OMB to develop a mechanism to analyze, track, and evaluate the risks and results of an agency's major capital investments in information systems. OMB will incorporate the criteria into future revisions of OMB Circular A-130. Further, OMB requires agencies to apply the criteria in conjunction with Memorandum M-97-02, "Funding Information Systems Investments," which emphasizes the need for well-justified budget requests.

As previously stated, the President intends that the United States take all necessary measures to swiftly eliminate any significant vulnerability to its critical infrastructures. Accordingly, unless

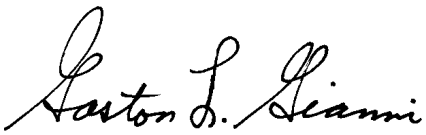
[9] The National Plan, issued by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism, is the first attempt by a national Government to design a way to protect its cyberspace.

additional funding is forthcoming, some agencies may need to reprioritize application of existing funding to meet PDD 63 requirements. Our suggestion to establish performance measures should provide the additional attention needed to ensure that funding is made available to implement PDD 63.

* * * * *

We appreciate your consideration of the matters discussed in this letter. If you have any questions or comments, please call Russell A. Rau, NASA Assistant Inspector General for Auditing, at (202) 358-4458.

Sincerely,



Gaston L. Gianni, Jr.
PCIE Vice Chair

Barry R. Snyder
ECIE Vice Chair

Enclosure

Identical letter directed to:
Mr. Richard Clarke
National Coordinator for Security, Infrastructure
Protection and Counter-Terrorism

Enclosure

PARTICIPATING OFFICES OF INSPECTOR GENERAL

Agency for International Development

Department of Agriculture

Department of Commerce

Department of Education

Department of Energy

Department of Health and Human Services

Department of Housing and Urban Development

Department of the Interior

Department of Justice

Department of State

Department of the Treasury

Federal Deposit Insurance Corporation

Federal Emergency Management Agency

Federal Reserve Board

General Services Administration

National Aeronautics and Space Administration

Nuclear Regulatory Commission

Office of Personnel Management

Railroad Retirement Board

Small Business Administration

Treasury Inspector General for Tax Administration