FINAL AUDIT REPORT

REVIEW OF TREASURY'S CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

OIG-01-025 December 14, 2000

Office of Inspector General

****

United States Department of the Treasury

December 14, 2000

MEMORANDUM FOR LISA ROSS
ACTING ASSISTANT SECRETARY (MANAGEMENT)
AND CHIEF FINANCIAL OFFICER

FROM: Dennis S. Schindel **/S/**
Assistant Inspector General for Audit

SUBJECT: Final Audit Report: Review of the Critical Infrastructure Protection Program

This memorandum transmits our Final Report on the *Review of the Critical Infrastructure Protection Program*. This audit was identified as a priority area in the Office of Inspector General's (OIG) Annual Audit Plan for Fiscal Year 2000. For this audit, we evaluated the progress made by the Department of the Treasury (Treasury), and its offices and bureaus, in implementing its Critical Infrastructure Protection Program for protecting its cyber-based systems.

We included three findings and three recommendations to assist Treasury in the implementation of Presidential Decision Directive (PDD) 63. Overall, our review found that Treasury is making reasonable progress towards fulfilling the cyber-related requirements of PDD 63 and the National Plan for Information Systems Protection Version 1.0, *Invitation to a Dialogue* (National Plan). However, improvements could be made to assist Treasury in fully implementing PDD 63 and to meet the deadlines imposed by the National Plan and PDD 63. Specifically, we noted that funding and resources to implement PDD 63 are inadequate and implementation oversight can be made more effective. In addition, Treasury needs to identify its critical infrastructure assets. A lack of detailed knowledge of Treasury-wide system assets may be viewed as a Federal Manager's Financial Integrity Act material weakness.

In response to our October 13, 2000, draft audit report, you agreed with the findings and provided actions responsive to our recommendations. Specifically, you indicated that your office completed the activity of identifying and prioritizing critical cyber assets via the National Critical Infrastructure Assurance Office (CIAO) on October 23, 2000. While we

consider these actions as tacit concurrence with the recommendations, you classified them as a non-concurrence as the desired actions had already been taken by the date of your response. We do not believe that any further action is needed on this issue.

For recommendation number three, however, the OIG does not agree with your planned timeframe established for updating the *Department of the Treasury Critical Infrastructure Protection Plan* (TCIPP), dated November 18, 1998. The TCIPP has not been updated to reflect the comments made by the Expert Review Team in the timeframes established by the National CIAO for the update. In addition, PDD 63 requires that the plan be updated every 2 years. The plan should be immediately updated to reflect the current status of the effort and should include revised timeframes for completion of the remaining tasks for both the cyber and non-cyber sides of the effort. Once the initial update is completed, the Department should revise the plan on a periodic basis as the effort evolves.

We appreciate the courtesies and cooperation provided to our staff during the audit. If you wish to discuss this report, you may contact me at (202) 927-5400, or a member of your staff may contact Clifford H. Jennings, Director, Office of Information Technology Audits at (202) 927-5771.

Attachment

EXECUTIVE DIGEST

Overview

Critical infrastructure protection (CIP) has become an important issue for the Federal Government. To address this issue, the Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63, issued May 1998, calls for a national effort to assure the security of the nation's critical infrastructures--also known as mission essential infrastructure (MEI[1]). Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government.

The intent of PDD 63 is that by May 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.
- The private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Our review found that the Department of the Treasury (Treasury) is making reasonable progress towards fulfilling the cyber-related requirements of PDD 63 and the National Plan for Information Systems Protection Version 1.0, *Invitation to a Dialogue* (National Plan), especially with the lack of funding and personnel resources directed towards the PDD 63 effort. The Treasury Office of Information Systems Security (OISS) established a Cyber CIP Working Group to implement the cyber aspects of PDD 63 and provided oversight and guidance to the bureaus to assist with the

[1] The National Chief Infrastructure Assurance Office (National 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."

identification of cyber Treasury critical infrastructures (TCI) [2] and the performance of vulnerability assessments to address PDD 63.

However, a significant amount of work remains to fully implement PDD 63. In particular, we identified that:

- Funding and resources to implement PDD 63 are inadequate.
- Treasury needs to identify its critical infrastructure assets.
- Implementation oversight can be made more effective for PDD 63.

Objective, Scope, and Methodology

The overall objective of this review was to determine whether Treasury and its offices and bureaus, were making reasonable progress in implementing the Treasury CIP Program for protecting its cyber-based systems. Our audit was conducted in participation with the President's Council on Integrity and Efficiency (PCIE) effort to conduct a government-wide review of the nation's critical infrastructure assurance program (CIAP).

To meet our objective, we reviewed the process used and guidance issued by OISS to coordinate, oversee, and implement PDD 63 at Treasury. In addition, we conducted fieldwork at the Office of Thrift Supervision (OTS), Financial Management Service (FMS), and the United States Secret Service (Secret Service) to determine the effectiveness of and compliance with OISS' PDD 63 effort.

Our audit was conducted from January 2000 through August 2000 at OISS, OTS, FMS and Secret Service. Further, we conducted interviews with officials at Corporate System Management for the Treasury Communications System, Office of Security, Comptroller of the Currency, and the National CIAO's Project Matrix Team.

[2] TCI will be used in place of MEI throughout the remainder of this report. TCI are defined as "A Treasury employee, system, or facility, the loss of which, either through destruction or incapacitation, would have a debilitating effect on the Department's ability to accomplish its major national security and economic security functions; continuity of government functions; and other essential government services. TCI are either owned or controlled by the Department or provided to the Department exclusively for its use."

EXECUTIVE DIGEST

The audit was performed in accordance with accepted *Government Auditing Standards*.

Recommendations and Management Response:

The Assistant Secretary (Management)and Chief Financial Officer should ensure that:

1. Funding and resources are made available to implement PDD 63.

2. Critical infrastructure assets are immediately identified and prioritized.

3. More effective oversight of PDD 63 implementation at Treasury is provided.

The Department's response to our draft report concurred with each of our findings and recommendations. Their response is summarized and evaluated in the body of the report and included in detail as Appendix 2, Management Response.

TABLE OF CONTENTS

AUDIT RESULTS

Background

Protection of critical infrastructures has become an important issue for the Federal Government. In October 1997, the President's Commission on Critical Infrastructure Protection issued its report calling for a national effort to assure the security of the United States' increasingly vulnerable and interconnected infrastructures. Advances in information technology have caused infrastructures to become increasingly automated and inter-linked, and have created new vulnerabilities to equipment failures, human error, weather, and physical and cyber attacks.[3] Non-traditional attacks on the Nation's information system infrastructures may be capable of significantly harming the economy and military power.

To address this issue, the Administration's Policy on Critical Infrastructure Protection: PDD 63, issued May 1998, calls for a national effort to assure the security of the nation's critical infrastructures--also known as MEI. Critical infrastructures are 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. PDD 63 requires that the Executive Branch assess the cyber vulnerabilities of the Nation's critical infrastructures--information and communications, energy, banking and finance, transportation, water supply, emergency services, and public health as well as those authorities responsible for the continuity of federal, state and local governments.

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 including especially its cyber systems. By May 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:

[3] Cyber attacks, or cyber terror, may be defined as the unauthorized electronic access, manipulation or destruction of electronic data or code that is being processed, stored or transmitted on electronic media, having the effect of actual or potential harm to the nation's critical infrastructure.

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

Each department and agency of the Federal government is responsible for protecting its own critical infrastructures, especially its cyber-based systems. Treasury is also designated Lead Agency for the Banking and Finance infrastructures. Each Treasury office and bureau is responsible for identifying TCI, assessing its vulnerabilities, and assuring its availability, integrity, survivability and adequacy. Protection plans were to have been developed for each Treasury office and bureau by November 1998, and implemented by May 22, 2000.

The National Plan revised the implementation date to December 2000. More specifically, the National Plan provides for a goal of achieving a critical information systems defense with an initial operating capability by December 2000, and a full operating capability by May 2003.

Objective, Scope, and Methodology

The overall objective of this review was to determine whether Treasury and its offices and bureaus, were making reasonable progress in implementing the Treasury CIP Program for protecting its cyber-based systems. To meet our objective, we reviewed the process used and guidance issued by OISS to coordinate, oversee, and implement PDD 63 at Treasury. In addition, we conducted fieldwork at OTS, FMS, and the Secret Service to determine the effectiveness of and compliance with OISS' PDD 63 effort.

The PCIE headed a government-wide effort to review the nation's CIAP. As a participant in this effort, we included the completion of review steps addressing the adequacy of Treasury's planning and assessment activities contained in the *PCIE/ECIE Review Guide, Phase I*, dated December 15, 1999. Specifically, the review guide

addressed the adequacy of agency plans, asset identification efforts, and the completion of initial vulnerability assessments for cyber-based infrastructures.

Our audit was conducted from January 2000 through August 2000 at OISS, OTS, FMS and Secret Service. Further, we conducted interviews with officials at Corporate System Management for the Treasury Communications System, Office of Security, Comptroller of the Currency, and the National CIAO's Project Matrix Team.

The audit work was performed in accordance with accepted *Government Auditing Standards*.

AUDIT RESULTS

Overview

This report presents the results of our audit to evaluate whether Treasury and its offices and bureaus, were making reasonable progress in implementing a CIP program for its cyber-based systems. We performed this review in conjunction with a review of the Nation's CIAP initiated by the PCIE.

Treasury began implementing PDD 63 requirements by completing the *Department of the Treasury Critical Infrastructure Protection Plan* (TCIPP), dated November 18, 1998. The TCIPP calls on each Treasury office and bureau to share responsibility for identifying TCI, assessing its vulnerabilities, and assuring its availability, integrity, survivability and adequacy. The plan states that "every effort will be made to build upon the strengths and expertise currently residing in Treasury's departmental offices and bureaus to adequately address this important national priority." For example, Treasury should build upon its Year 2000 (Y2K) efforts to identify its mission critical systems and contingency planning when addressing PDD 63.

Our review found that Treasury is making reasonable progress towards fulfilling the cyber-related requirements of PDD 63 and the National Plan, especially given the lack of funding and personnel resources directed towards the PDD 63 effort. OISS' Cyber CIP Program Manager (Program Manager) organized the establishment of the Cyber CIP Working Group to implement the cyber aspects of PDD 63. Through the Cyber CIP Working Group forum, the Program Manager has provided oversight and guidance to the bureaus to assist with the identification of cyber TCI and the performance of vulnerability assessments to address PDD 63. For example, OISS issued the *Department of the Treasury Cyber Critical Infrastructure Protection Implementation Plan, Version 1.0* (Implementation Plan), which provides a methodology for implementing cyber CIP at Treasury. Currently, OISS is organizing the National CIAO's Project Matrix effort, which will assist with the completion of the cyber TCI identification and prioritization.

However, while Treasury overall has made progress towards implementing a CIP Program for its cyber-based systems, we found that a lot of work remains to fully implement PDD 63 and to meet

the deadlines imposed by the National Plan and PDD 63. In particular, we identified that:

- Funding and resources to implement PDD 63 are inadequate.
- Treasury needs to identify its critical infrastructure assets.
- Implementation oversight can be made more effective for PDD 63.

Finding 1: Funding and Resources to Implement PDD 63 Are Inadequate

Treasury has not adequately funded its current PDD 63 effort and has not ensured that future funding to implement PDD 63 will be available. Further, Treasury does not have sufficient personnel resources fully devoted to carry out the requirements of PDD 63. Due to the lack of adequate funding and resources for PDD 63 implementation, Treasury cannot ensure that the risks resulting from security weaknesses (i.e., inadequate access and system software controls identified during the performance of vulnerability assessments) will not discontinue the services it provides, such as revenue collection, law enforcement, and financial management. In addition, Treasury cannot ensure that attacks on its cyber critical infrastructures will not hinder its support of National Security, National Economic Security, and National Public Health and Safety.

Details

Treasury does not currently have adequate funding dedicated to carry out PDD 63 requirements and has not taken the steps necessary to ensure that future PDD 63 efforts are properly funded. In addition, Treasury currently lacks the full-time resources needed to fully implement PDD 63. The lack of funding and resources to implement PDD 63 is a major concern for OISS and the bureaus we reviewed.

Department-wide Funding

For Fiscal Year (FY) 2000, Treasury provided base-line funding for PDD 63 by reprogramming $1 million to carry out various aspects of

its PDD duties, including PDD 63. The funds were distributed between the Office of Financial Institutions Policy, the Treasury Chief Information Officer (CIO), and the Office of Security. The Treasury CIO's portion of the reprogramming effort was not adequate to cover cyber CIP program expenses for the year. In addition, the reprogramming effort did not include any funding support for the bureaus to begin implementing PDD 63.

Treasury, and its bureaus, without further reprogramming, will not have adequate funding in FY 2001 to perform vulnerability assessments on PDD 63 critical assets and to develop remediation plans to correct identified vulnerabilities. For FY 2001, no specific funding for PDD 63 was included in the Treasury budget request to the Office of Management and Budget (OMB). Any bureau requests to the Department for PDD 63 funding were removed from the Treasury direct appropriation submission to OMB. Specifically, the Secretary of the Treasury (Secretary) withheld funding requests for government-wide mandates, such as PDD 63, from the budget submission. The Secretary's position is that PDDs are external issues and that OMB should provide funding for these initiatives. Further, because there is limited funding available for Treasury's direct appropriation, Treasury is unable to financially address these important issues. In recognition of OMB's leadership in ensuring government-wide coordination and success, the Secretary requested further White House and OMB collaboration on funding approaches to fulfill PDD requirements.

As a potential source of funding for PDD 63, Treasury was informed that OMB was initially planning to provide $25 million in passback for Treasury's Counterterrorism Fund in December 1999. The passback justification provided that these funds should be used, as necessary, to address the externally mandated program demands surrounding PDDs and Continuity of Operations related activities. OISS was hopeful that some of this $25 million passback would be used to assist the cyber PDD 63 effort at both the Department and bureau levels.

In May 2000, the Counterterrorism Fund passback was increased to $55 million, however, the justification for use of the funds was revised and no longer included specific funding for PDDs. The revised justification stated that funding was designated as a

contingent emergency appropriation to cover unanticipated costs. The funds would only be available under emergency conditions and could not be used for ordinary events that could be planned for, such as the implementation of protective measures to address PDD 63.

An additional concern for future PDD 63 funding is that neither the Treasury CIO nor the Treasury Capital Investment Review Board (CIRB) is ensuring that proper budgeting for PDD 63 requirements occurs. The Treasury CIO did review the FY 2001 budget submissions and provided feedback to the bureaus on information technology areas requiring attention. However, emphasis on PDD 63 was not included in these comments. In addition, the Treasury CIRB has not discussed the need for planning for PDD 63 funding with the bureaus when reviewing Treasury information technology initiatives. We also found that while the Department issued guidance to the bureaus on how to formulate budget submissions, no specific policy guidance was provided on specific areas of importance for which the bureaus should budget, such as PDD 63.

According to an OMB official, for FY 2001 and possibly beyond, agencies should not plan to receive supplemental funding from OMB for PDD 63 efforts, as was the case for Y2K. OMB's stance is that information security is not a new initiative and that agencies should have been budgeting all along for addressing their system security needs. OMB basically views PDD 63 as an identification and prioritization effort that underscores interconnectivity. After the identification and prioritization is complete, information security requirements already in existence should cover the remainder of what PDD 63 intends. While OMB correctly asserts that PDD 63 should have been previously funded under existing computer security requests, Treasury has not previously funded the PDD 63 effort and needs to raise the level of funding for computer security issues overall.

Further, beginning with FY 2002 budget submissions, OMB will not consider new or continued funding for system investments that do not meet the criteria outlined in OMB Memorandum M-00-07, *Incorporating and Funding Security in Information Systems Investments*, dated February 28, 2000. The memorandum provides criteria for agencies to incorporate and fund security into its

information systems investments and architectures and tie these needs into business operations.

The memorandum includes six principles that "…will support more effective agency implementation of both agency computer security and critical information infrastructure protection programs. In terms of Federal information systems, critical infrastructure protection starts with an effort to prioritize key systems…Once systems are prioritized, agencies apply OMB policies…to achieve adequate security commensurate with the level of risk and magnitude of likely harm." The memorandum also includes five criteria that must be included in budget proposals, beginning with FY 2002, for investments in the development of new or existing information systems, both general support systems and major applications.

Cyber CIP Program Funding

Specific to the cyber CIP program, the National Plan requires Federal agencies to adopt a multi-year funding plan to remedy assessed vulnerabilities by December 2000. In addition, OISS issued guidance to the bureaus for developing budget submissions for PDD 63 in the Implementation Plan, dated April 24, 2000. Specifically, Section 5.6, *Cyber CIP Budget Guidance*, indicates that budget submissions should address the resources required to support the program (i.e., personnel, equipment), the metrics used to determine the cost of the program, training requirements, and whether the effort can be supported internally or if it requires contractor support. The guidance further states that each cyber CIP program should cover a five-year period and address all issues that may be expected to surface during the program life cycle.

To date, Treasury and its bureaus have not defined a multi-year funding plan to fully implement the cyber CIP program. The Program Manager has been working towards determining the funding needs of OISS and the bureaus to continue PDD 63 efforts, such as perform vulnerability assessments and interdependency analyses, in anticipation of receiving some of the passback funding discussed above. However, based on the revised justification for the passback, OISS can no longer depend on the use of Counterterrorism Funds to support PDD 63 requirements. While not specific to PDD 63, we did find that that OISS' and the bureaus funding requirements address

information systems security in general, such as Public Key Infrastructure and network security.

The National Plan states that "...success in meeting the milestones established in the National Plan will depend upon the level of funding provided." However, because of the Secretary's view that OMB should provide funding for PDD 63 and OMB's view that agencies should be properly budgeting for information security and protection of critical infrastructures, uncertainty exists for PDD 63 funding for FY 2002 and beyond.

Limited Personnel Resources

In addition to the lack of funding for PDD 63, there are also limited resources devoted to PDD 63. At the time of our review, the Program Manager, along with two contractors, were the only resources devoted to cyber CIP implementation at the Department level. On the physical side, the Acting Deputy Director, Office of Security, is working on PDD 63 part-time and no full-time resources are assigned this responsibility.

We also found that while those resources that are assigned to PDD 63 are information security personnel, the bureaus do not have the resources devoted full-time to the cyber-side of PDD 63. We found this to be the case at the three bureaus we reviewed: OTS, Secret Service, and FMS. For example, FMS was unable to assign dedicated positions to the critical infrastructure initiative. However, FMS "pooled" its existing resources and expertise across the organization, which enabled FMS to fully participate in critical infrastructure activities, such as attending Cyber CIP Working Group meetings and answering data calls. Secret Service also does not have any full-time resources devoted to PDD 63. What limited resources the Secret Service has available will be directed toward implementing information security measures, in general, rather than on documenting the process, policies, etc.

Additionally, Treasury has not completed its identification and prioritization of TCI (see Finding 2). Until the identification and prioritization is complete, Treasury cannot adequately determine budget estimates for funding and plan for resources to perform vulnerability assessments and remediation plans on the most critical

PDD 63 related assets. Further, Treasury needs a completed TCI identification and prioritization to focus what resources are available on those assets that most strongly support the National level.

Due to the lack of adequate funding and resources for PDD 63, Treasury cannot ensure that potential risks resulting from security weaknesses (i.e., inadequate access and system software controls identified during the performance of vulnerability assessments) will not discontinue the services it provides for the government, such as revenue collection, law enforcement, and financial management. In addition, Treasury cannot provide the necessary assurance that cyber attacks on its PDD 63 critical infrastructures will not impede its support of National Security, National Economic Security, and National Public Health and Safety.

Recommendation 1:

The Assistant Secretary (Management) and Chief Financial Officer should ensure that funding and resources are made available to implement PDD 63. Specifically:

- Ensure that PDD 63 funding is incorporated into future budget submissions. Funding requests for information security and critical infrastructure protection should be adequately justified and tied to Treasury and bureau missions as mandated by OMB.
- Ensure that necessary funding and resources are provided to assess vulnerabilities and develop remediation plans for critical TCI.

Management Response:

The Department concurred with this recommendation. The OISS developed a FY 2002 business case for the CIRB upon which to establish appropriated funding for departmental information security and cyber CIP requirements. In addition, Treasury bureaus are to baseline their Information Technology (IT) security posture and then determine a desired (or target) IT security posture utilizing the *Treasury Step 1 Project Matrix Report* and the cyber CIP framework.

Office of Inspector General (OIG) Comment:

The Department's planned corrective actions meet the intent of our recommendation.

Finding 2: Treasury Needs to Identify Its Critical Infrastructure Assets

While Treasury has made progress towards implementing a CIP program for its cyber-based systems, the identification of cyber TCI assets for PDD 63 has not been completed. Until Treasury has identified the TCI that meets the intent of PDD 63, Treasury cannot ensure that vulnerabilities are fully assessed and that remediation plans are developed to protect its critical infrastructures that support its core business functions (i.e., revenue collection, law enforcement, and financial management), in addition to its support of National Security, National Economic Security, and National Public Health and Safety.

Details

Treasury is still in the process of identifying its cyber-based TCI assets for PDD 63. The identification effort began in November 1998, with the issuance of the TCIPP by the Treasury CIO and Critical Infrastructure Assurance Officer (CIAO). The TCIPP provided directions and the profile format for the Departmental Offices and bureaus to follow in inventorying their information systems. In March 1999, the Treasury CIAO requested all bureau TCI profiles to be completed by May 14, 1999. In August 1999, the Treasury CIO extended the due date for the completion of the inventories to September 3, 1999.

Although each of the bureaus submitted their profiles, OISS found that the profiles basically provided Y2K information and stated that some were more complete than others. For example, the Bureau of Engraving and Printing's profile was detailed, per the instructions contained in the March 1999, memo from the CIAO, and included the TCI name, type of infrastructure, function supported, owner/operator, location, point of contact, priority and impact due to loss/degradation. The Departmental Office's initial TCI profile was

less detailed and only included the name of the system, type of system, function supported, owner, office, and priority. While Y2K was a good basis for the bureaus to begin the identification effort, further refinement of the profiles was needed to address PDD 63 requirements (i.e., National Security, National Economic Security, and National Public Health and Safety).

In November 1999, the Cyber CIP Working Group held its first meeting and has since been the vehicle for the implementation of the cyber aspects (i.e., hardware, software, communications systems) of PDD 63, with the Program Manager overseeing and guiding the effort. In January 2000, to continue the refinement process, the Program Manager, with the assistance of two contractors, began meeting with each bureau to discuss the identification process, validate data requirements, learn about the bureaus' particular environment, identify existing inventories, and note any concerns or issues the bureaus had with the CIP initiative.

After these meetings, the bureaus were to continue refining their initial profile submissions as described in the Implementation Plan, dated February 22, 2000, and in subsequent versions of the Implementation Plan. The bureaus provided OISS with specific profile information that included: bureau name; core business function; Executive Order 12656, *Assignment of Emergency Preparedness Responsibilities*, function supported; system name; priority level as defined in the TCIPP and Implementation Plan; and interdependencies with other bureaus and agencies. OISS planned to use this information to assist with the TCI identification and prioritization effort and to begin populating a centralized database of PDD 63 related infrastructures.

In March 2000, OISS and the Cyber CIP Working Group began discussing the need for an additional level of profile detail. This additional level would contain specific system information, such as hardware configuration, operating systems, and application software. OISS presented, to the Cyber CIP Working Group and the CIO Council, the need for the information as useful to manage/oversee and track the status of the critical infrastructure assets, the CIP program, and computer security programs within Treasury. The additional level would also benefit compliance/review activities,

Treasury's Computer Security Incident Response Capability (CSIRC) implementation, and risk management. To date, the bureaus have not provided this additional level of detail.

While OISS obtained updated TCI profiles from all the bureaus, less the additional level of detail, the process of identifying cyber TCI has been slow. The bureaus expressed concern with OISS over the definition of critical assets. For example, the bureaus we reviewed felt that Treasury was focused more on systems rather than on business functions and that they were rehashing the information of critical systems that was previously provided under the criteria for Y2K. The bureaus also contend that most of their systems do not meet the National definition of critical asset and that OISS did not provide the bureaus with a clear definition of how the loss of their asset would have a debilitating effect on the Nation. Further, the bureaus were unclear as to the definition of what CIP is as compared with what is required in OMB Circular A-130, *Management of Federal Information Resources*.

Treasury bureaus also had concerns with the need for the additional level of detail being requested by OISS (i.e., the specific system information including hardware configuration, operating systems, and application software). According to the bureaus we reviewed, OISS has not provided a clear understanding of the need for this information, how the data would be used, and how security over the data would be provided.

Further hindering the efforts to identify cyber TCI has been the manual process used by OISS to gather this data from the bureaus. OISS had initially planned to develop and populate a database with the information obtained through the PDD 63 effort to provide Treasury with a reporting capability (i.e., assessments, interdependencies) for this initiative. OISS provided an overview of the benefits of a cyber CIP database during individual meetings with the bureaus. Some of the benefits to be derived by the bureaus were to: assist with regulatory compliance; provide efficient response to advisories; and record the status of remediation activities. However, the bureaus have expressed concern to both the Treasury CIO and OISS regarding the ownership of and security over the information. In addition, the bureaus feel their systems will become more vulnerable when all of the data collected on Treasury critical

infrastructures is stored in one location. In reference to these concerns, the Treasury CIO informed the CIO Council on February 10, 2000, that the database would not be pursued.

The Treasury CIO, however, needs specific information to effectively oversee and manage the implementation of PDD 63, in addition to other information system and security requirements. For example, under the Information Technology Management Reform Act, the Treasury CIO is responsible for ensuring that Treasury information security policies, procedures, and practices are adequate and that a Treasury information system architecture is developed. In an effort to comply with this requirement, a Treasury Information Systems Architecture Framework (TISAF) is being developed and will include system information, such as the hardware and software on which bureau applications are running. Other components of the TISAF will include: applications and system services; communications interfaces and services; and interfaces with external and external systems.

The TISAF may not, however, meet the needs of the Treasury CIO to manage other information technology requirements. OMB A-130, *Management of Federal Information Resources*, Appendix III, *Security of Federal Automated Information Resources*, requires the Treasury CIO to implement and maintain a program to assure adequate security. For PDD 63, the Treasury CIO is responsible for providing the information assurance of cyber-based information systems. Also, OISS' current effort to develop a Treasury CSIRC will provide Treasury with a mechanism to disseminate computer security incident information Department-wide and a consistent capability to respond to, and report on, computer security incidents in support of PDD 63.

While initial efforts were being made to identify TCI, Treasury is currently using the National CIAO's Project Matrix team for the identification and prioritization of its critical assets that support the National level. As of July 5, 2000, Project Matrix had identified 135 Treasury systems as potential PDD 63 assets but the National CIAO's *Infrastructure Asset Evaluation* survey needed to be completed to further refine the assets for PDD 63 purposes.

The Project Matrix effort will provide a basis for Treasury to prioritize its critical assets and focus vulnerability and remediation efforts on those most critical assets that support the National level intent of PDD 63. In addition, both the second level of the TCI profile detail and a centralized database could provide the Treasury CIO with an efficient and effective means of tracking Treasury progress in implementing PDD 63, as well as other information system and security requirements.

Until Treasury completes its identification and prioritization of TCI that address PDD 63, Treasury cannot fully assess information systems vulnerabilities, adopt a multi-year funding plan to remedy them, and create a system for continuous updating by December 2000. In addition, failure to identify and properly evaluate Treasury critical assets could result in the discontinuation of vital services Treasury provides in support National Security, National Economic Stability, and National Public Health and Safety, in addition to its core functions (i.e., revenue collection, law enforcement, and financial management).

Recommendation 2:

The Assistant Secretary (Management) and Chief Financial Officer should ensure that critical infrastructure assets are immediately identified and prioritized. Specifically:

- Ensure Treasury completes its identification of TCI and prioritize those assets that support PDD 63 in order to assess vulnerabilities and request adequate funding for remediation efforts.
- Ensure the Treasury CIO obtains the information necessary to manage and oversee all of Treasury information technology efforts, in addition to satisfying requirements specific to PDD 63 to support the development of a Department-wide database of Treasury information systems. The Treasury CIO should be responsible for determining the level of detail necessary to carry out these efforts and provide for adequate security over the database.

Management Response:

The Department concurred with the recommendation and noted that the completion of its identification and prioritization of TCI that support PDD 63 was accomplished via the National CIAO on October 23, 2000. The Department concurred with the recommendation for developing a Department-wide database of Treasury information systems. The design, development, and implementation of this requirement is proposed for FY 2002, or earlier if funding becomes available.

OIG Comment:

While not completed at the time of our review, the OIG agrees that the National CIAO's effort at Treasury assisted the Department in the completion of the identification and prioritization of TCI assets and meets the intent of the recommendation. In addition, we agree with the Department's intended actions to develop a Department-wide database of information systems.

Finding 3: Implementation Oversight Can Be Made More Effective for PDD 63

While Treasury has established an organizational structure for implementing and administering PDD 63, Treasury has not integrated and coordinated the implementation of both the cyber and non-cyber aspects of PDD 63. In addition, the role of the Treasury Infrastructure Protection Panel (TIPP) in this effort has been underutilized and has not carried out its roles and responsibilities for the Treasury-wide PDD 63 effort. Therefore, Treasury cannot ensure that all TCI, including non-cyber assets that protect critical cyber assets, are identified and that protective measures are in place to prevent intrusions causing the disruption of service to support, not only its core missions, but also National Security, National Economic Security, and National Public Health and Safety.

Details

Treasury developed an organizational structure to implement PDD 63. The Secretary designated responsibility to the Treasury CIO and the CIAO to implement the requirements of PDD 63. The

Treasury CIAO is responsible for the protection of the non-cyber based infrastructures, and the Treasury CIO for providing information assurance of cyber-based information systems. Both the Treasury CIO and CIAO co-chair the TIPP which is comprised of representatives from each bureau, usually the bureau CIO and CIAO. The TIPP was established to facilitate and coordinate the implementation and institutionalization of a comprehensive CIAP.

On the cyber side, the Treasury CIO tasked OISS with management responsibility for the Department-wide Cyber CIP Implementation. The Program Manager is responsible for coordinating the actions of the various Treasury bureaus and Departmental Offices supporting this effort. A Cyber CIP Working Group was formed to be the main vehicle to accomplish the Treasury mandate to develop and maintain a plan for protecting the Treasury cyber critical infrastructures. The Cyber CIP Working Group includes representatives from each Treasury bureau with the Program Manager designated as Chair. The Office of Security is responsible for the implementing the physical side of PDD 63. The Cyber CIP Organization is shown in Appendix 1 of this report.

However, the TIPP has not been actively involved in the implementation of PDD 63 nor has it provided adequate guidance and oversight, as described in its roles and responsibilities, to the PDD 63 efforts being made.

The roles and responsibilities of the TIPP, as outlined in the TCIPP, include:

- Developing and assigning responsibilities for implementing a comprehensive CIAP to implement the TCIPP.
- Developing, formulating, and recommending for approval, and establishment by the Department, policies and guidelines such that all mission-essential functions shall continue effectively and without interruption in the face of attacks (both physical and cyber) on TCI.
- Promoting organizational relationships and lines of communication necessary to ensure that Treasury bureaus have the capability to carry out their assigned responsibilities in the protection of the TCI.

- Acting as a forum for the dissemination of information pertaining to state-of-the-art technologies, products, and practices for ensuring critical infrastructure assurance.
- Providing guidance as needed to departmental offices and bureaus, to include TCI element identification and reporting, Risk Statements, Penetration Testing, Security Test and Evaluation and Risk Management.

The Implementation Plan adds an additional responsibility for the performance of interdependency analysis when Departmental Offices and bureaus identify the TCI elements and interfaces.

Integration and Coordination of Cyber and Non-Cyber

While no judgments are being made as to the implementation of the non-cyber aspects of PDD 63, we found that there has been minimal communication and integration between the cyber and non-cyber sides to implement PDD 63. Both OISS and the bureaus have expressed concern over the lack of involvement and guidance issued by the non-cyber side. One bureau official indicated that the facilities, utilities, and personnel that support the core business processes are at least equally as important as the cyber assets. In response to the bureaus' concerns regarding the status of the implementation of the physical side for PDD 63, OISS has attempted to integrate the effort by inviting the non-cyber counterpart to the Cyber CIP Working Group meetings and including these individuals on all PDD 63 related correspondence with the working group members. In addition, some of the bureaus have initiated their own effort to integrate both the cyber and physical sides of PDD 63 at the bureau level to ensure that both sides are fully informed of progress made and that all critical assets are identified and protected.

While the implementation of the physical aspects of PDD 63 was outside the scope of this review, we found that the Office of Security prefers to meet with the bureaus one-on-one to address non-cyber vulnerability assessments. The Office of Security has not issued any specific guidance to the bureaus for implementing the physical side of PDD 63. However, as outlined in the TCIPP, the Director of Security is responsible for integrating the policies established by the TIPP for non-cyber TCI elements into policy guidance and standards. The Office of Security is providing input into the current Project

Matrix effort to address non-cyber, however, the Office of Security is meeting directly with the Project Matrix team and does not plan to coordinate this effort with OISS.

While the Office of Security and the Treasury CIO's office did originally coordinate the development of the TCIPP in 1998, the TCIPP has not been revised to reflect comments from the National CIAO's Expert Review Team nor updated to reflect the current status of Treasury's PDD 63 effort. According to the Program Manager, the Office of Security updated the TCIPP to address physical infrastructures, however, the cyber portion of the plan has not been updated. Within the Treasury CIO's office, the individual responsible for developing the cyber portion of the TCIPP has not updated the plan because he does not believe that the TCIPP should be updated until Treasury has sufficient funds to actually implement PDD 63.

The Program Manager stated that OISS would be willing to update the cyber portion of the TCIPP, but in the meantime, has developed supplemental guidance to address the cyber critical infrastructures and has developed internal cyber vulnerability assessment guidance. However, the only Treasury guidance that coordinates both the cyber and non-cyber PDD 63 efforts, the TCIPP, is outdated and needs to be revised. The TIPP, which should be overseeing both the cyber and non-cyber efforts and promoting the development of guidance, has not ensured the update of the TCIPP.

Oversight and Guidance

The Program Manager has been overseeing and providing guidance to the Cyber CIP Working Group for the cyber aspects of PDD 63. For example, the Program Manager and a contractor developed, and OISS issued, the *Department of the Treasury Cyber Critical Infrastructure Protection (CIP) Guidance and Methodology for Conducting Vulnerability and Risk Assessments, Version 1.0*, dated May 31, 2000.

Our review, however, found that vulnerability assessment guidance already in existence would have been adequate to address the needs for PDD 63. The vulnerability assessment methodology described in the guidance issued by OISS is essentially the same as the guidance in

the TCIPP. In addition, the National CIAO's *Practices for Securing Critical Information Assets*, dated January 2000, also provides guidance for addressing vulnerability assessments. Appendix C of the document provides information on the National Security Agency's information systems security (INFOSEC) Assessment Methodology (IAM) developed to provide assistance to PDD 63 departments and agencies in assessing their INFOSEC postures. The IAM is a National CIAO-endorsed methodology that could be used as a baseline standard for cyber vulnerability analysis.

According to the Program Manager, there was a need to develop new guidance because other guidance did not address interdependencies or provide for an interdependency analysis. Our review of the newly issued guidance showed that only one page was included in the guidance with a general discussion on interdependency analysis. The guidance also included a list of tools available for conducting cyber CIP vulnerability/risk assessments.

The TIPP has met only once, on April 21, 1999, throughout the process of implementing PDD 63 at Treasury. The TIPP is co-chaired by the Treasury CIO and CIAO and its members are the bureau CIOs and CIAOs. Additionally, for seven of the 17 bureaus and Departmental Offices that make up the TIPP, the CIO is also the CIAO. Many of the TIPP participants are also on the Treasury CIO Council in which discussions on issues and concerns over PDD 63 cyber efforts take place. The Treasury CIO has encountered problems gaining the consensus of the bureau CIOs on PDD 63 issues, such as the centralized database of critical assets. The TIPP is an even larger group, again with many of the same participants of the CIO Council. Therefore, the current size and structure of the TIPP may be too large to productively facilitate, coordinate, and make decisions regarding the implementation of PDD 63 at Treasury.

Additionally, because the TIPP has met only once, there has been no integrated means of discussing and making decisions regarding the development and formalization of guidance; the assignment of responsibilities for implementing the TCIPP; the promotion of organizational relationships and lines of communications; and involvement in the performance of an interdependency analysis between the cyber and non-cyber sides. Further, had the TIPP been involved in the process of reviewing and recommending guidance to

implement PDD 63, already limited resources may have been better utilized. Regarding the vulnerability assessment guidance, both the section on interdependency analysis and the listing of vulnerability assessment tools could have been provided to the bureaus as supplements to the TCIPP, and external guidance, without Treasury incurring the expense of having a contractor develop a new guidance document. Also, any guidance that has been issued, with the exception of the TCIPP, is geared towards the cyber-based TCI and does not incorporate the non-cyber TCI.

For the cyber PDD 63 effort, the Program Manager reports directly to the Director, OISS, and is also required to report to the CIO, the TIPP, and the CIO Council. The Program Manager has reported the status of the PDD 63 cyber efforts to the CIO Council throughout the process but has not directly reported to the TIPP on the process for identifying TCI, the performance of vulnerability assessments, or planned remediation efforts for identified vulnerabilities. As the TIPP has met only once, it has not provided direct supervision over the Program Manager for the implementation of the cyber aspects of PDD 63.

It is imperative that the TIPP provide a strong and integrated oversight role to both the cyber and non-cyber efforts. Improving the oversight role is becoming even more critical given the amount of effort remaining and the limited resources available to implement PDD 63 at Treasury. For example, improved oversight is particularly critical where known vulnerabilities of non-cyber TCI protecting the cyber TCI are not integrated and coordinated. The lack of a strong and integrated oversight role may result in Treasury having to face additional risks (i.e., intrusions), which may cause the disruption of service which not only support core missions but also National Security, National Economic Security, and National Public Health and Safety.

Recommendation 3:

The Assistant Secretary (Management) and Chief Financial Officer should ensure more effective oversight of PDD 63 implementation at Treasury. Specifically:

- Ensure that both the cyber and non-cyber aspects of PDD 63 are coordinated and integrated at both the Departmental and bureau level. This could be accomplished through the auspices of the TIPP.
- Require the TIPP to reassess its current organizational structure to ensure that it can effectively and productively facilitate and coordinate the implementation and institutionalization of the CIAP. In addition, the TIPPs roles and responsibilities should be strengthened to ensure that adequate supervision and guidance over implementation of PDD 63 at Treasury is provided to OISS and the Office of Security.
- Ensure that the TCIPP, dated November 1998, is immediately updated to reflect the National CIAO's Expert Review Team comments and the current status of cyber and physical PDD 63 efforts at Treasury.

Management Response:

The Department concurred with our recommendation to integrate and coordinate the cyber and non-cyber aspects of PDD 63 at both the Departmental and bureau level. The Office of Security was realigned under the Deputy Assistant Secretary (Information Systems) and CIO on October 1, 2000; an IT Security Focus Group was recently formed; membership responsibilities of the TIPP will be addressed on/before January 2001; and the TIPP shall be scheduled to meet on a quarterly basis beginning January 2001.

The Department concurred with the intent of our recommendation for the TIPP to reassess its current organization structure to ensure the facilitation and coordination needed to implement the CIAP and ensure that adequate supervision and guidance to OISS and the Office of Security. The Department did not agree with the insinuation that OISS has been inadequate in its efforts to put forth viable and reasonable operational guidance.

Finally, the Department agreed with the need to update the TCIPP, however, the update is predicated on funding and is scheduled to be completed by September 2001.

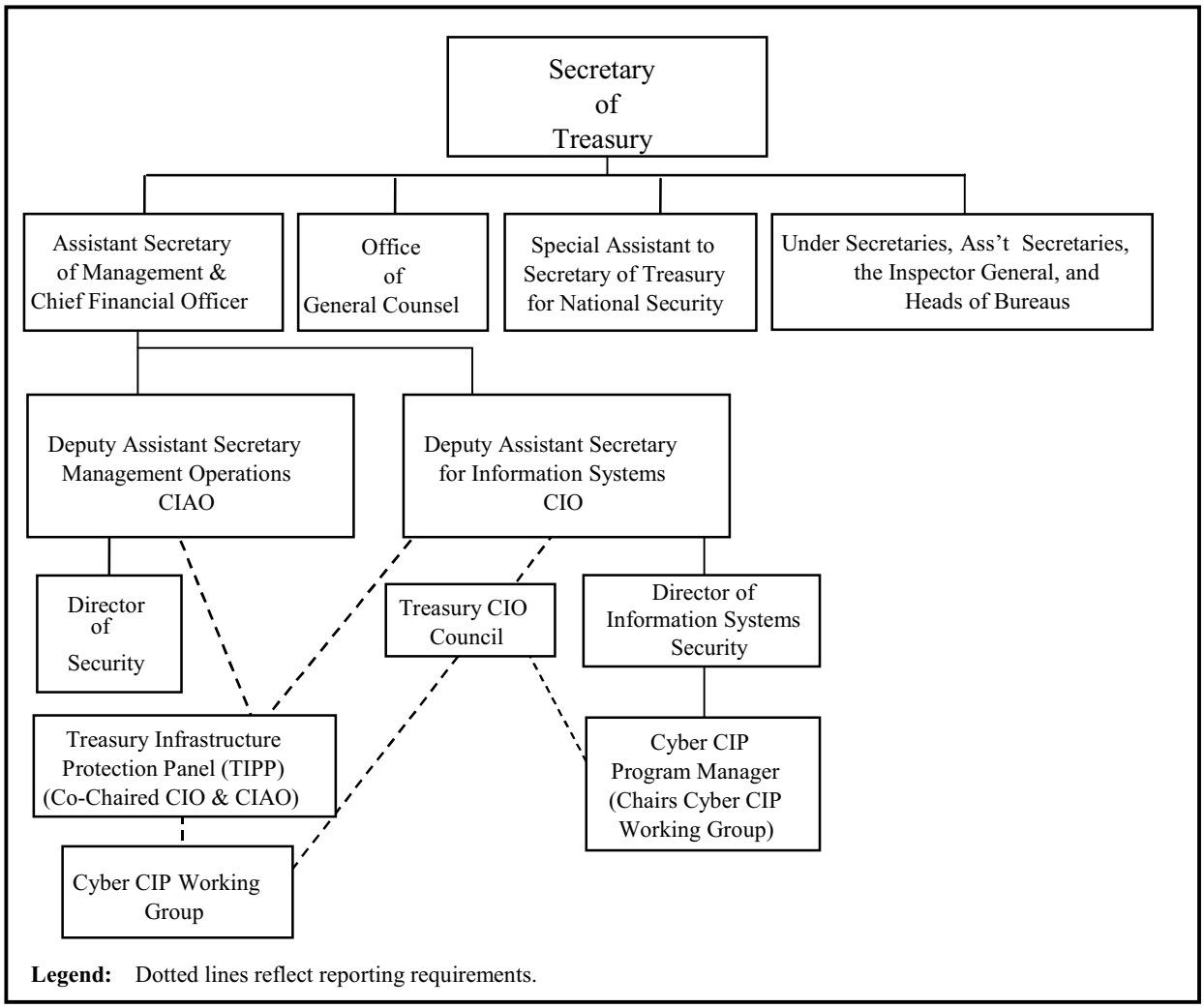
OIG Comment:

The OIG agrees with the intent of the planned actions for integrating and coordinating the cyber and non-cyber aspects of PDD 63 at the Departmental and bureau level. The OIG does not agree with the planned timeframe established for updating the TCIPP. The TCIPP has not been updated to reflect the comments made by the ERT in the timeframes established by the National CIAO for the update. In addition, PDD 63 requires that the plan be updated every two years. The plan should be immediately updated to reflect the current status of the effort and should include revised timeframes for completion of the remaining tasks for both the cyber and non-cyber sides of the effort. Once the initial update is completed, the Department should revise the plan on a periodic basis as the effort evolves.

With regard to the Department's non-concurrence with the insinuation that OISS has been inadequate in its efforts to put forth viable and reasonable operational guidance, it was not the OIG's intent to insinuate that OISS' efforts have been inadequate. It is the OIG's opinion that OISS has made significant progress with regards to implementing the cyber side of PDD 63. However, the TIPP is responsible for acting as a forum for the dissemination of information pertaining to state-of-the-art technologies, products, and practices for ensuring critical infrastructure assurance and providing guidance as needed to the Department and bureaus. The example used in the report states that guidance already existed for vulnerability assessments that could have been utilized by OISS. Had the TIPP been involved in the PDD 63 effort, it could have recommended that OISS issue supplements to the existing guidance that address new areas of focus, such as interdependency analysis or tools available for conducting vulnerability assessments, especially given the lack of funding currently available for this effort. The Department did, however, agree with the intent of this recommendation and should develop corrective actions to address this issue.

CYBER CIP ORGANIZATION

The Department of the Treasury Cyber CIP Organization as provided in the *Department of the Treasury Cyber CIP Implementation Plan, Version 1*.3, dated April 24, 2000.



Legend: Dotted lines reflect reporting requirements.

MANAGEMENT RESPONSE

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

ASSISTANT SECRETARY

NOV 13 2000

MEMORANDUM FOR DENNIS S. SCHINDEL
ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Lisa Ross
Acting, Assistant Secretary (Management)
and Chief Financial Officer

SUBJECT: Draft Audit Report: Review of the Critical Infrastructure Protection Program

The Chief Information Office submits the attached responses in reference to the Draft Audit Report: Review of the Critical Infrastructure Protection Program dated October 13, 2000. The attached documentation represents comments and corrective actions for your consideration.

Attachments

MANAGEMENT RESPONSE

CIO Response to Draft Audit Report:
Review of Critical Infrastructure Protection (CIP) Program

As requested, concurrence (to include a written summary of corrective actions, and estimated completion) or non-concurrence (with written explanation) on the recommendations and findings of the subject draft audit report are provided as follows.

Finding 1, Recommendation 1:

"The Assistant Secretary for Management and Chief Financial Officer should ensure that funding and resources are made available to implement PDD 63."

- We concur with this finding. Requirements for implementing PDD 63 include: 1) the identification of Treasury critical infrastructure (TCI), 2) the development of Departmental operational guidance on Information Technology (IT) security related activities, 3) the implementation of this operational guidance by bureaus, 4) the development and implementation of a departmental management/oversight capability, and 5) the provision of funding and resources for implementation.

- Treasury critical infrastructure has been identified by the National Critical Infrastructure Assurance Office (CIAO). This information is documented in the Treasury Step 1 Project Matrix Report dated October 23, 2000.

- The Department has issued operational guidance for the performance of various CIP-related IT security activities. This guidance has been developed and coordinated with the bureaus. Collectively, this operational guidance represents a framework for the bureaus to use in implementing cyber CIP requirements. A critical component of the framework is the departmental IT Security Roadmap which is under development. It shall be used by the bureaus in planning long-term operational IT security improvements. The roadmap is scheduled for completion by February 2001.

- The Office of Information Systems Security has recently developed a FY 2002 business case for the Capital Investment Review Board (CIRB) in which to establish appropriated funding for departmental information security and cyber CIP requirements. One of the proposed requirements in the business case is the design, development, and implementation of a management/oversight capability for cyber CIP. The CIRB is scheduled to meet and review the business case in November 2000.

- Using the Treasury Step 1 Project Matrix Report and the cyber CIP framework (in particular the IT Security Roadmap), bureaus shall baseline their IT security posture and then determine a desired (or target) IT security posture. The target IT security posture shall be the basis for the bureaus to strategically plan their future IT security improvement activity, resources, and funding over a multiple year period. This activity to baseline and target IT security posture by each bureau is scheduled to

MANAGEMENT RESPONSE

occur in March 2001. An outcome of this activity shall be the development of the bureau's cyber CIP Management Plan. Using these plans, the Department will be postured to pursue Corporate Funding Initiatives in future years when requirements are common among the bureaus or a need exists that can benefit the enterprise overall.

Finding 2, Recommendation 2:

"The Assistant Secretary for Management and Chief Financial Officer should ensure that critical infrastructure assets are immediately identified and prioritized. Specifically:

Ensure Treasury completes its identification of TCI and prioritize those assets that support PDD 63 in order to assess vulnerabilities and request adequate funding for remediation efforts."

- We non-concur with this aspect of the recommendation. As stated in Finding 1, this activity was accomplished via the National CIAO on October 23, 2000.

"Ensure the Treasury CIO obtains the information necessary to manage and oversee all of Treasury information technology efforts, in addition to satisfying requirements specific to PDD 63 to support the development of a Department-wide database of Treasury information systems. The Treasury CIO should be responsible for determining the level of detail necessary to carry out these efforts and provide for adequate security over the database."

- We concur with this finding. The Office of Information Systems Security (OISS) recognizes this as a critical component of the cyber CIP program. OISS has made several efforts to accomplish this; however, the bureaus were very negative about providing this information. The design, development, and implementation of this requirement is proposed for FY 2002, or earlier if funding becomes available.

- The findings and recommendations of this audit shall be scheduled for discussion by the TIPP either on November 21, 2000, or at the next meeting (January 2001.)

Finding 3, Recommendation 3:

"The Assistant Secretary for Management and Chief Financial Officer should ensure more effective oversight of PDD 63 implementation at Treasury. Specifically:

Ensure that both the cyber and non-cyber aspects of PDD 63 are coordinated and integrated at both the Departmental and bureau level. This could be accomplished through the auspices of the TIPP."

- The Office of Security was realigned under the Deputy Assistant Secretary (Information Systems) and Chief Information Officer on October 1, 2000. A new IT

MANAGEMENT RESPONSE

security structure, encompassing all security disciplines, shall be in place by January 1, 2001.

- The Treasury CIO Council recently formed an IT Security Focus Group co-chaired by the TIPP CIAOs for IRS and FMS with oversight by the senior Department IT Security Manager. This triumvirate would be ideally suited to oversee bureau and Department integration and implementation of IT security requirements while ensuring oversight and compliance for PDD 63.

- The membership and responsibilities of the TIPP shall be addressed on/before January 2001.

- The TIPP shall be scheduled to meet on a quarterly basis commencing January 2001.

"Require the TIPP to reassess its current organizational structure to ensure that it can effectively and productively facilitate and coordinate the implementation and institutionalization of the CIAP. In addition, the TIPPs role and responsibilities should be strengthened to ensure that adequate supervision and guidance over implementation of PDD 63 at Treasury is provided to OISS and the Office of Security."

- While we concur with the intent of this recommendation, we non-concur on the insinuation that OISS has been inadequate in its efforts to put forth viable and reasonable operational guidance. OISS has been very proactive in providing specific guidance on implementing IT security requirements, in identifying TCI data, and in addressing how this data can be used by the Treasury CIO in management, oversight, and compliance of CIP, and in support of the Department Computer Security Incident Response Capability. Where possible, OISS has addressed non-cyber requirements.

"Ensure that the TCIPP, dated November 1998, is immediately updated to reflect the National CIAO's Expert Review Team comments and the current status of cyber and physical PDD 63 efforts at Treasury."

- We concur with the need to update this strategic guidance. The update of the TCIPP is predicated on funding and is scheduled to be completed by Sep 2001.

ABBREVIATIONS

CIAO	Chief Infrastructure Assurance Officer
CIAP	Critical Infrastructure Assurance Plan
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIRB	Capital Investment Review Board
CSIRC	Computer Security Incident Response Capability
FMS	Financial Management Service
FY	Fiscal Year
IAM	Information Systems Security Assessment Methodology
Implementation Plan	*Department of the Treasury's Cyber Critical Infrastructure Protection Plan*
INFOSEC	Information Systems Security
IT	Information Technology
MEI	Mission Essential Infrastructure
National CIAO	National Critical Infrastructure Assurance Office
National Plan	National Plan for Information Systems Protection Version 1.0, *Invitation to a Dialogue*
OIG	Office of Inspector General
OISS	Office of Information Systems Security
OITA	Office of Information Technology Audits
OMB	Office of Management and Budget
OTS	Office of Thrift Supervision
PCIE	President's Council on Integrity and Efficiency
PDD	Presidential Decision Directive
Program Manager	Cyber CIP Program Manager
Secret Service	United States Secret Service
Secretary	Secretary of the Treasury
TCI	Treasury Critical Infrastructure
TCIPP	*Department of the Treasury Critical Infrastructure Protection Plan*, dated November 18, 1998
TIPP	Treasury Infrastructure Protection Panel
TISAF	Treasury Information Systems Architecture Framework
Treasury	Department of the Treasury
Y2K	Year 2000

MAJOR CONTRIBUTORS TO THIS REPORT

Office of Audit

Clifford Jennings, Director, Office of Information Technology Audits (OITA)
Edward Coleman, Deputy Director, OITA
Melinda Smith, IT Auditor-in-Charge
Michael DiDiego, IT Auditor
Catherine Fudge, IT Auditor
Michael Stein, Referencer

REPORT DISTRIBUTION

The Department of the Treasury

Acting Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems and Chief Information Officer
Deputy Assistant Secretary for Management Operations
Director, Office of Information Systems Security
Program Manager, Cyber CIP
Commissioner, Financial Management Service
Director, United States Secret Service
Director, Office of Thrift Supervision
Comptroller, Comptroller of the Currency
Director, Corporate Systems Management
Office of Accounting and Internal Control, Departmental Offices

Office of Management and Budget

Office of Inspector General Budget Examiner

Other

President's Council on Integrity and Efficiency