FINAL REPORT ON THE REVIEW OF TREASURY COMPUTER SECURITY PLANS

OIG-01-014 November 2, 2000

Office of Inspector General

****

Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

OFFICE OF
INSPECTOR GENERAL

November 2, 2000

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

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

SUBJECT: Final Report on the Review of Treasury Computer Security Plans

This memorandum transmits our Final Report on the Review of Treasury Computer Security Plans. The overall objective of this audit was to determine whether the Department of the Treasury (Treasury) has developed computer security plans that will ensure that the information in Treasury computer systems is protected against loss, misuse, or unauthorized access and modification.

We included two findings with recommendations to assist Treasury in improving the computer security plans. First, the Deputy Assistant Secretary for Information Systems (DASIS)/Chief Information Officer (CIO) needs to update the Treasury-wide policies and guidance for the development of computer security plans and ensure that the Treasury bureaus' security plans comply with current regulations. In addition, the CIO needs to develop security plans for systems of the Departmental Offices (DO). These plans should address the current system vulnerabilities identified and be kept up-to-date. The CIO also needs to develop an information systems inventory for systems he is responsible for managing.

We found that the Office of the DASIS/CIO has taken initial steps to update the agency-wide system security guidance and to identify the vulnerabilities in the DO systems. However, in your September 27, 2000, response to our draft report you did not fully concur with our findings. We have added comments at the end of the report dealing with these issues and the methods you believe mitigate some of the problems noted. We call your attention to Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Section A.3.3, which requires you to "…consider identifying a

deficiency pursuant to OMB Circular A-123, *Management Accountability and Control* and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan or no authorization to process for a system." We suggest you consider identifying the lack of computer security plans for the identified DO systems as deficiencies per OMB Circular A-130.

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 Jennings, Director, Office of Information Technology Audits at (202) 927-5771.

Attachment

EXECUTIVE DIGEST

Overview

In the present day business environment, organizations rely on automated information systems to accomplish their missions. Federal Government agencies are required by law to protect their systems and the information processed and stored. While the Department of the Treasury (Treasury), Office of the Deputy Assistant Secretary for Information Systems/Chief Information Officer (CIO) has made some efforts to secure its systems, a significant amount of work remains to be completed.

We reviewed the Treasury system security policies and guidance issued to the bureaus to assist them in their development of computer security plans. We found that while the CIO recently issued security guidance in some limited high-risk security areas, updated system security planning guidance that complies with the current regulations released within the last several years has not been issued. In addition, the CIO is not performing oversight of the bureaus to determine if they are developing adequate system security plans.

We also evaluated the security plans for the information systems within the Departmental Offices (DO). For these systems, we found that although the CIO is performing assessments to identify the vulnerable areas in its system security, adequate security plans have not been developed and all systems may not have been identified in the DO systems inventory listing.

Although the CIO has taken some initial steps to ensure the protection of Treasury systems, additional actions are needed in order for the CIO to obtain the necessary level of assurance that all systems are adequately secure. Without the appropriate controls, Treasury systems and the information contained on its systems are vulnerable to loss, misuse, and unauthorized disclosure or modification.

Objectives, Scope and Methodology

The overall objective of our audit was to determine whether Treasury has developed computer security plans in order to ensure that its systems are protected from harm. We determined if the CIO was providing adequate guidance and oversight to ensure that the bureaus' have developed security plans to protect their systems. In addition, we determined if the CIO had developed system security plans for DO systems.

To accomplish our objectives, we interviewed personnel from the CIO's Office. We also reviewed Treasury system security policies and examined

the security plans for DO automated information systems. The fieldwork was performed from February 2000 to July 2000. The audit was performed in accordance with *Government Auditing Standards*.

Recommendations and Management's Response:

The Treasury Chief Information Officer should:

1) Update system security planning guidance to reflect current regulations.
2) Ensure that periodic reviews are conducted of the bureaus' security plans.
3) Correct system vulnerabilities identified in DO systems, update DO system security plans, and ensure through the Certification and Accreditation process that system security plans are kept up-to-date and that new system vulnerabilities are identified and addressed.
4) Develop a means to identify all existing and newly implemented DO systems.

Treasury's September 27, 2000, response to our draft concurred with our first finding and recommendations (items 1 and 2 above).

Treasury's response to our draft report did not fully concur with our report recommendations (items 3 and 4 above) to resolve the second finding. Their response is summarized and evaluated in the body of this report and included in detail as Appendix 1, Management Response.

TABLE OF CONTENTS

EXECUTIVE DIGEST

INTRODUCTION

Background 1

Objective, Scope and Methodology 2

AUDIT RESULTS

Overview 2

Finding 1: Treasury-wide Security Program Needs to be Strengthened 3

Recommendations 6

Finding 2: The Departmental Offices Needs to Strengthen Controls Over Systems Security 7

Recommendations 8

APPENDICES

Appendix 1: Management Response 11

Appendix 2: Abbreviations 15

Appendix 3: Major Contributors to this Report 16

Appendix 4: Report Distribution 17

AUDIT RESULTS

Background

The Department of the Treasury (Treasury) spends approximately $2 billion annually for Information Technology (IT) operations. Treasury IT systems contain and process a vast array of critical and sensitive data supporting Treasury and government-wide operations as well as services to the American public. Treasury bureaus and offices are enhancing these systems to provide more customer-oriented services utilizing advancing technologies such as e-commerce which introduce new risks and vulnerabilities. Consequently, the information processed and stored on Treasury systems is susceptible to the risk of loss, misuse, or unauthorized disclosure from outside attacks such as terrorist and hackers, inadvertent errors or intentional acts by insiders, and natural disasters.

In the Treasury Information Technology Strategic Plan for the years 2000-2003, security is part of the foundation of Treasury's IT strategic direction. In line with this principle, Treasury needs to ensure that its systems are appropriately protected in order for Treasury to accomplish its mission and to protect the privacy rights of U.S. citizens. Treasury's mission cuts across several significant areas which include managing the government's finances, protecting the financial system and our nation's leaders, and fostering a safe and drug-free America. The successful accomplishment of Treasury's mission affects important Treasury operations such as the collection of over ninety-eight percent (98%) of the government's revenue as well as the continuity of government-wide operations.

Recognizing the threats and vulnerabilities of its systems, the Federal Government has taken actions in an attempt to protect itself in this area. Several statutes including the Computer Security Act of 1987, the Information Technology Management Reform Act (a.k.a. "Clinger-Cohen") of 1996, and the Paperwork Reduction Act of 1995, require the identification of computer security risks and the development of computer security standards and plans. In addition, the Office of Management and Budget (OMB) Circular No.A-130, *Management of Federal Information Resources*, and the National Institute of Standards and Technology (NIST) Special Publication 800-18, *Guideline for Developing Security Plans for Information Technology Systems*, provide guidance for implementing security programs and developing security plans.

Succeeding the Year 2000 computing crisis, the Congress is refocusing its attention to systems security. On November 19, 1999, a bill proposing the Government Information Security Act of 1999 was introduced by the Senate Governmental Affairs Committee. The bill was unanimously approved by

the Senate Governmental Affairs Committee on March 23, 2000. In addition to requiring agencies to develop and implement security policies and control techniques, the bill includes a provision that will require an annual independent evaluation of security programs and practices.

Objective, Scope, and Methodology

The overall objective of this review was to determine whether Treasury has developed computer security plans in order to ensure that the information in Treasury computer systems is protected against loss, misuse, or unauthorized access and modification. We reviewed whether the CIO has provided guidance and standards to assist the bureaus in the development of computer security plans, and if the CIO is ensuring that the bureaus' security plans are current and viable. In addition, we reviewed whether the CIO has developed adequate computer security plans to protect DO automated systems.

To accomplish these objectives, we interviewed CIO officials. We reviewed Treasury Directives (TD) pertaining to the development of information systems security plans and policies and for the oversight of the bureaus' security programs. We also evaluated the security plans for DO automated information systems. Fieldwork was performed from February 2000 to July 2000. The audit was performed in accordance with *Government Auditing Standards*.

Overview

In recent years, organizations have grown to depend on automated information systems in order to fulfill their missions. The Federal Government has recognized the importance of its systems and has issued regulations requiring agencies to protect the information stored and processed by these systems. Treasury has made efforts to address some of these new requirements by issuing updated agency-wide guidance covering timely, vulnerable areas such as Internet security and the usage of gateways and firewalls. In addition, the CIO is currently having a contractor perform risk assessments for DO systems. The risk assessments will be used by the system owners to develop action plans addressing the vulnerabilities identified and eventually to update the system's security plans.

We evaluated TDs issued by the CIO providing the bureaus with guidance in the development of system security plans. We also evaluated the CIO's procedures to ensure the bureaus' compliance with this guidance.

We found that the Treasury guidance requiring the bureaus to develop security plans has expired and did not reflect current legislation. We also

found that the CIO is not performing oversight of the bureaus to ensure that adequate system security programs are established including the development of system security plans. After examining the security plans within DO, we found that they did not have adequate system security plans for its own systems and may not have identified all systems in its inventory.

Treasury has made some initial efforts to develop a current agency-wide security program and to protect the systems within DO. However, a significant amount of work still remains in the area of security plans in order for Treasury to have assurance that all of the agency systems are protected against loss, misuse, or unauthorized access and modification. As a result, the CIO needs to update Treasury security plan guidance, provide oversight of the bureaus, and strengthen the controls over the security of the systems within DO.

Finding 1. Treasury-Wide System Security Program Needs to be Strengthened

The CIO has not issued updated guidance to the Treasury bureaus and offices for the development of security policies and plans. In addition, the CIO does not perform oversight of the Treasury bureaus and offices to ensure that the bureaus' security policies and plans are current and viable. As a result, Treasury does not have assurance that its bureaus and offices are adequately protecting their systems by instituting sufficient security programs and by developing systems security plans which are viable and compliant with current regulations.

System Security Planning Guidance Is Out-of-Date

The guidance issued by the CIO to assist the bureaus in the development of system security plans has not been updated to reflect the requirements contained in recent legislation. As a result, the bureaus do not have current system security planning standards to refer to when updating and developing their system security plans.

The most current guidance issued by the CIO is based upon OMB Bulletin 90-08, dated July 9, 1990. This bulletin provided only initial security planning guidance and has since been superseded. The Treasury systems security plan guidance dates back to July 1994, and requires the documentation of only general system information. The guidance also further directs the functional system owner to prepare computer security plans for new systems under development which contain sensitive information. Based upon the 1994 guidance, security plans are required to be updated during the testing phase and at the conclusion of each risk assessment or other significant system change. The guidelines also include a standard format to assist the bureaus in this task. The format suggested by

the Treasury guidance does not require the documentation of the system security requirements and details describing the security controls in place or planned. Instead, the system owner is required to determine general system information such as the system description, components (i.e., modules and subsystems), status (i.e., operational or under development), category (i.e., application, LAN, processing center), type of data processed, kind of network access, and risk assessment schedule. However, the Treasury security plan format does not require the system owners to include details about the system security controls such as management controls (i.e., rules of behavior), operational controls (i.e., physical protection, data integrity/validation controls, security awareness and training), or technical controls (identification and authentication, logical access controls, audit trails).

One of the current Federal regulations requiring agencies to develop system security plans is OMB Circular A-130, dated February 8, 1996. OMB Circular A-130 instructs agencies to follow the guidance issued by NIST for developing system security plans. In December 1998, NIST issued Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems", for Federal agencies to follow as a model for its computer security plans.

The CIO has not updated its system security plan guidance to reflect current Federal regulations because its efforts have been focused on updating its policies on the issues (i.e., Internet security and firewalls) that it determined to be the most critical to the security of the agency. Although these issues are important to system security, this limited focus has left other significant areas neglected. According to a project schedule, the CIO plans to update its system security guidelines by September 2000.

The CIO has not provided updated guidance on the development of security plans. As a result, the bureaus are not receiving the necessary level of assistance in order to develop adequate system security plans. Currently, the bureaus' plans do not consistently comply with the current regulations and some of the bureaus have not developed security plans at all. Without security plans which include the necessary level of detail required by Federal regulations, the CIO can not determine if Treasury systems are adequately protected.

The Oversight of Bureau System Security Planning Could Be Improved
The CIO is not providing oversight and assistance to the bureaus in their development of computer security plans. As a result, Treasury can not be assured that the Treasury bureaus are developing system security plans and complying with security planning regulations.

The CIO's oversight and bureau assistance procedures include the performance of security reviews at four bureaus annually. During these reviews, the effectiveness of the bureaus' security is to be evaluated in areas such as personnel, physical/environmental, information systems, and emergency preparedness. The CIO performed one of these reviews at the U.S. Secret Service in May 1999; however, no additional reviews have been accomplished.

The Treasury Security Manual assigns the CIO the responsibility for reviewing and approving the bureaus' system security policies and computer system security plans. The current Federal regulations requiring agencies to develop system security programs are included in OMB Circular A-130 and the Computer Security Act of 1987. Specifically, OMB Circular A-130 requires that Federal agencies implement and maintain a program to assure that adequate security is provided for its systems. OMB Circular A-130 defines adequate security as, "security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls."

The CIO has not complied with its plan to perform security reviews at the bureaus due to the lack of staffing. However, a recent reorganization of the CIO's office presents an opportunity for it to reinstitutionalize the security review process.

Due to the lack of bureau oversight, the CIO does not have assurance that the Treasury bureaus are following system security planning regulations and developing system security plans. In addition, the CIO does not have assurance that the bureaus are identifying system vulnerabilities and taking the actions necessary to protect its systems and the information contained in these systems from being compromised.

AUDIT RESULTS

Recommendations

The Treasury Chief Information Officer should:

1. Update system security planning guidance to reflect current regulations, and
2. Ensure that periodic reviews are conducted of the bureaus' security plans.

Management Response:

The Treasury CIO fully concurred with the finding and presented a Corrective Action Plan to address recommendations.

OIG Comment:

The OIG agrees that the steps to be taken by the CIO will correct the noted weaknesses.

AUDIT RESULTS

Finding 2. The Departmental Offices Needs to Strengthen Controls Over Systems Security

Up-to-date systems security plans have not been developed for DO automated information systems. The security plans currently on-file are significantly out-of-date and inadequate. In addition, while the CIO is responsible for the DO systems inventory, there is no process to ensure that the inventory is complete and accurate. As a result, the CIO does not have assurance that system vulnerabilities have been identified and that appropriate actions have been taken in order to adequately protect its systems.

Security plans were developed for some of DO's systems. However, the plans are obsolete and date back to 1991. These system security plans consist of a questionnaire type of report which attempts to answer general system questions such as the system status, the type of sensitive data handled by the system, the system operator, system interconnections, and system certification. While this information is important, the plans do not contain information found to be critical in the development of present day security plans such as authentication controls and data integrity and validation controls.

The Information Systems Security Section (ISSS) within the CIO has not been able to keep the DO systems inventory accurate and current. No formal process exists which notifies ISSS when new DO systems are implemented. ISSS attempts to identify new systems through the examination of budget submissions and maintenance requests. However, this process has proved ineffective since additional systems, which did not appear on the most current inventory listing, were discovered and identified through recent Critical Infrastructure Protection Program efforts.

The most current DO system inventory listing is dated March 15, 2000. This list ranks DO systems in order of risk priority. It also includes other pertinent information including the system owner, sensitivity level, system status (archive, operational, being replaced, or planned), and the date of the last risk assessment and when the next risk assessment is scheduled to be completed. However, the list does not indicate when the security plan for each system is scheduled to be updated.

The Federal regulations, OMB Circular A-130 and the Computer Security Act of 1987, both require agencies to develop system security plans. While the Computer Security Act of 1987 requires security plans for only sensitive systems, OMB Circular A-130 recognizes the need to go further and

requires the protection of all Federal systems. Within the CIO, the ISSS is responsible for ensuring that DO system owners develop security plans for its automated systems.

Security plans for DO systems have not been updated in a timely manner due to the lack of funding and personnel. ISSS has not been able to perform the Certification and Accreditation (C&A) process in which system security plans are supposed to be reviewed. If completed, the C&A process would ensure that security plans exist for each system and are up-to-date. ISSS has only been able to accredit two DO systems, and these accreditations need to be revisited as they date back to 1995. Recently, ISSS has taken initial steps to update its security plans by obtaining a contractor's assistance in performing risk assessments for all its systems. ISSS plans for these risk assessments to be completed by the end of fiscal year 2000. In addition, ISSS plans to obtain a contractor to develop security plans in fiscal year 2001 if funding is approved.

Because DO does not have adequate security plans for any of its known systems, the CIO can not be assured that the sensitive information processed by these systems is appropriately protected against unauthorized access, loss, or misuse. In addition, the CIO may not be considering additional resources needed in its efforts to update and accredit computer security plans if it is unaware of existing systems not currently included in the DO systems inventory.

Recommendations

The Treasury Chief Information Officer should:

Correct system vulnerabilities identified in DO systems, update DO system security plans, and ensure through the Certification and Accreditation process that system security plans are kept up-to-date and that new system vulnerabilities are identified and addressed.

Develop a means to identify all existing and newly implemented DO systems.

Management Response:

The Treasury CIO did not fully concur with the finding. While the Treasury CIO did acknowledge that DO security plans are not current, the CIO believes that measures have been taken to provide assurances that systems are protected against loss, misuse, or unauthorized access. The Treasury CIO indicated that certain procedures have addressed system vulnerabilities to include completion of risk assessments on nearly all DO systems processing sensitive data; penetration tests on systems determined to be most critical; completion of vulnerability assessments on the most critical systems using automated vulnerability assessment tools; and, development of risk mitigation plans for each risk assessment.

OIG Comment:

As a result of management's response, the OIG met with the Departmental Office IT Security to obtain clarification regarding the measures which the CIO reported as having been taken. The OIG was informed that IT Security had identified 10 major applications and four general support systems and had established a schedule for system security plan development. These 14 security plans are to be finished by December 31, 2002. The OIG noted IT Security previously had identified 71 systems and is taking steps for the preparation of security plans for the above 14 leaving 57 systems to be addressed. IT Security must ensure that each of the remaining systems is included as part of the security plans for the general support systems.

Further, as reported in management's response, two penetration tests were performed. The penetration test on the DO firewall was performed in December 1999, and the penetration test on the Cash Track System was not performed until September 2000, after our review. In addition, the vulnerability assessment using an automated tool was not performed until September 2000, also after our review.

The Treasury CIO stated that "Although Departmental Offices IT Security does not have updated security plans for every system, the measures taken to date do provide assurances that our systems are protected against loss, misuse, or unauthorized access." However, it is the system owner that must be provided the assurance that the systems are safe to operate. OMB A-130, Appendix, III, Section A.a.4 requires that a management official authorize in writing the use of each general support system based on implementation of its security plan. Therefore, without a current security plan, the system owner can not be assured that a system is safe to operate. Further, OMB A-130, Section A.3.3, requires that a deficiency be considered pursuant to

OMB Circular A-123, *Management Accountability and Control* and the Federal Managers' Financial Integrity Act (FMFIA), if there is not assignment of security responsibility, no security plan or no authorization to process for the system." As computer security plans are required to authorize the systems per OMB A-130, the OIG suggests that Treasury consider identifying the lack of computer security plans for the identified DO systems as deficiencies per OMB Circular A-130.

MANAGEMENT RESPONSE

DEPARTMENT OF THE TREASURY
WASHINGTON

ASSISTANT SECRETARY

SEP 27 2000

MEMORANDUM FOR DENNIS S. SCHINDEL, ASSISTANT INSPECTOR GENERAL FOR AUDIT

FROM: Lisa Ross
Assistant Secretary for Management and Chief Financial Officer

SUBJECT: Draft Audit Report: Review of Treasury Computer Security Plans

The Chief Information Office submits the attached responses in reference to the Draft Audit Report: Review of Treasury Computer Security Plans dated August 22, 2000. The attached documentation represents comments and corrective actions for your consideration.

Attachments

MANAGEMENT RESPONSE

CIO Response to Draft Audit Report:
Review of Treasury Computer Security Plans

The Treasury Chief Information Officer fully concurs with the following findings as stated in the Draft Audit Report: Review of Treasury Computer Security Plans dated August 22, 2000. The Office of the Inspector General found that the Treasury Chief Information Officer should "ensure that the guidance pertaining to system security planning is updated to reflect recent regulations", and that "periodic reviews are conducted of the bureaus' security plans." In addition, it was found that "system security plans must be updated along with a means to identify all existing and newly implemented Departmental Offices (DO) systems." Furthermore the "Certification & Accreditation (C&A) process must be re-instituted to ensure that security plans are kept up-to-date, and to address any new system vulnerabilities." We concur with these findings and the Corrective Action Plan is as follows:

- **Corrective Action Plan for Updating Guidance:**
  - The Office of Information Systems Security will issue an interim policy letter on security plan guidance for sensitive general support systems and major applications in October 2000.
  - Certification and accreditation policy and procedures are included in the revision of chapter 6 of TD P 71-10. Telos is under contract to develop a Treasury security architecture. This architecture and a proposed revised outline for chapter 6 are due by December 2000. The drafting of the new and revised policies and procedures will require approximately one year. Coordination and implementation of these policies will follow.
  - The Office of Information Systems Security (OISS) will submit the compliance review policy for official signature by September 30, 2000.
  - Reviews of bureau security plans will begin in FY 2001.
- **Corrective Action Plan for Updating Security Plans and Re-instituting Certification and Accreditation Process :**
  - The C&A process includes risk assessment; preparation of system security plans; security testing and evaluation of the system; certification that the controls are in place and evaluation of any residual risks; and written authority to operate. OMB Circular A-130 requires this be done at least every three years. C&A is a labor-intensive process. DO has fourteen major applications and general support systems. Each requires an average of three months to complete the entire process.

1

MANAGEMENT RESPONSE

- OISS/DO Security has developed a three-year plan to certify and accredit all DO major applications and general support systems. This plan will create the cycle of C&A required by the OMB Circular and will distribute the workload.

- **Corrective Action Completed to Provide the DO IT Security Team with the Inventory of Existing and Planned Systems:**

  - CIO/Automated Systems Division (ASD) has implemented a configuration management process to identify all existing and newly implemented DO systems. This process will provide the DO IT security team with the inventory of existing and planned systems.

The Treasury Chief Information Officer does not fully concur with the following findings as stated in the Draft Report:

- The Office of the Inspector General reported in Finding 2, page 5, "The Department Needs to Strengthen Controls Over Systems Security."

  - **Clarification Requested.** We concur with the overall finding. However, a clarification of the wording is requested. As worded, the finding appears to apply to the entire Treasury Department rather than the Departmental Offices. We are requesting that the wording for Finding 2 be changed to read; "The Departmental Offices Needs to Strengthen Controls over Systems Security."

- The Office of the Inspector General found that a "significant amount of work still remains in the area of security plans in order for Treasury to have assurance that all of the agency systems are protected against loss, misuse, or unauthorized access and modification." In addition, the IG recommends that "actions are taken to address the system vulnerabilities identified in risk assessments."

  - **The Treasury Chief Information Officer does not concur** with the above verbiage. As stated, the language directly ties the lack of having security plans in the agency to a lack of assurance that all of the agency systems are protected against loss, misuse, or unauthorized access and modification. Although Departmental Offices IT Security does not have updated security plans for every system, the measures taken to date do provide assurances that our systems are protected against loss, misuse, or unauthorized access.

  - Secondly, the following procedures were in place at the time of the review, to address system vulnerabilities identified in risk assessments.

2

MANAGEMENT RESPONSE

- Departmental Offices IT Security has conducted risk assessments on nearly all Departmental Offices (DO) systems processing sensitive data. The few exceptions are those that are being redesigned for later implementation. DO based the assessments conducted on the security requirements of OMB Circular A-130, TD P 71-10, Computer Security Act, DO security requirements and best practices for protecting sensitive systems. In the last 12 months, Departmental Offices IT Security has completed 30 separate risk assessments and has developed risk mitigation plans for reducing security risks to an acceptable level.

- Departmental Offices IT Security has conducted penetration tests on those systems determined to be most critical to ensure that controls established for those systems are indeed effective.

- Departmental Offices IT Security recently completed a vulnerability assessment on the most critical system in DO using automated vulnerability assessment tools.

- For every risk assessment, Departmental Offices IT Security has developed risk mitigation plans for reducing security risks to an acceptable level. Offices under the CIO are currently implementing these plans.

3

LIST OF ABBREVIATIONS

C&A	Certification and Accreditation
CIO	Office of the Deputy Assistant Secretary for Information Systems/Chief Information Officer
DO	Departmental Offices
ISSS	Information System Security Section
IT	Information Technology
NIST	National Institute of Standards and Technology
NIST 800-18	NIST Special Publication 800-18, *Guideline for Developing Security Plans for Information Technology Systems*
OMB	Office of Management and Budget
OMB A-130	OMB Circular A-130, *Management of Federal Information Resources*
TD	Treasury Directive
Treasury	Department of the Treasury

MAJOR CONTRIBUTORS TO THIS REPORT

Clifford Jennings, Director, Office of Information Technology Audits
Ed Coleman, Deputy Director, Office of Information Technology Audits
Catherine Fudge, IT Auditor
Chuck Intrabartolo, Computer Specialist
Kevin Burke, Referencer

REPORT DISTRIBUTION

Treasury Departmental Offices

Assistant Secretary for Management and Chief Financial Officer
Deputy Assistant Secretary for Information Systems and Chief Information Officer
Director for Information Systems Security
Chief of Information System Security Section

Office of Management and Budget

Esther Rosenbaum, Budget Examiner