The Internal Revenue Service Should Improve Actions to Protect Its Critical Infrastructure

June 2000

Reference Number: 2000-20-097

INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 19, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - The Internal Revenue Service Should Improve Actions to Protect Its Critical Infrastructure

This report presents the results of our review of the Internal Revenue Service's (IRS) actions to protect its critical infrastructure. We conducted this review in conjunction with other similar audits being performed by members of the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. At least 21 Inspectors General are participating in the project.

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63, dated May 1998, calls for a national effort to assure the security of the nation's critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and government, such as telecommunications, banking and finance, energy, and transportation.

In summary, we found that, although the IRS has taken significant actions to identify and correct security weaknesses in recent years, only limited actions have been initiated to formally address critical infrastructure protection planning and assessment requirements. If the IRS' critical infrastructure is not adequately evaluated, the government's primary revenue collector, and other agencies and states that use its data, could be at risk of disrupted operations and processing delays.

We issued a draft of this report to IRS management on April 28, 2000, with a May 30, 2000, response period. However, management's response was not available as of the date this report was released.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions,

or your staff may call Scott Wilson, Associate Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Table of Contents

Executive Summary

The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63, dated May 1998, calls for a national effort to assure the security of the nation's critical infrastructure. The infrastructure includes systems essential to the minimum operations of the economy and government, such as telecommunications, banking and finance, energy, and transportation.

PDD 63 requires that each government department and agency prepare a plan for protecting its own critical infrastructure. The objective of this review was to evaluate the adequacy of the Internal Revenue Service's (IRS) planning and assessment activities for protecting its critical computer-based infrastructure. We conducted this review in conjunction with other similar audits being conducted by members of the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. At least 21 Inspectors General are participating in the project.

Results

During the last three years, the IRS has taken significant actions to identify and correct security weaknesses. These actions have included conducting extensive on-site security reviews of IRS facilities and some systems. While it is likely that these reviews have covered many mission essential systems, the IRS has taken only limited actions to formally address the required deliverables asked for in PDD 63.

The Internal Revenue Service Has Taken Limited Actions to Address Critical Infrastructure Planning and Assessment Requirements

The IRS appointed a Chief Infrastructure Assurance Officer (CIAO) in December 1999, and has assigned a limited staff for support. However, little has been done to meet the first milestones prescribed by PDD 63: to identify all mission essential assets, ensure that complete vulnerability assessments for these specific assets have been performed, and develop a multi-year funding plan for managing the critical infrastructure program by December 2000. As a result, these milestones are in jeopardy of not being met. Until mission essential assets are defined and steps are taken to ensure that each of these assets has been adequately evaluated, IRS management will not have a complete accounting of the vulnerabilities of its critical infrastructure or a clear picture of the actions necessary to comply with PDD 63.

If the IRS' critical infrastructure is not adequately evaluated, the government's primary revenue collector, and other agencies and states that use its data, could be at risk of disrupted operations and processing delays.

Summary of Recommendations

To expedite efforts to meet the PDD 63 milestones, the IRS should use the results of its ongoing security evaluation efforts, which are identifying and correcting security weaknesses, in actions to comply with PDD 63. Additionally, the IRS CIAO should coordinate with senior Department of the Treasury and IRS officials to expedite the definition and identification of mission essential assets for critical infrastructure protection.

Management's Response: We issued a draft of this report to IRS management on April 28, 2000, with a May 30, 2000, response period. However, management's response was not available as of the date this report was released.

Objective and Scope

The objective of this review was to evaluate the IRS' planning and assessment activities for protecting its critical computer-based infrastructure.

This review was conducted in conjunction with other similar audits being conducted by members of the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency. At least 21 Inspectors General are participating in the project.

The overall review will consist of four phases and is designed to evaluate the adequacy of the federal government's critical infrastructure protection program. Phases I and II relate to the critical computer-based infrastructure; and Phases III and IV relate to the critical physical infrastructure. Our objective in Phase I was to evaluate the adequacy of the Internal Revenue Service's (IRS) planning and assessment activities for protecting its critical computer-based infrastructure.

To accomplish our objective, we interviewed the IRS Chief Infrastructure Assurance Officer (CIAO) and personnel in the Department of the Treasury. In addition, we reviewed guidelines and direction contained in *The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive (PDD) 63,* dated May 1998; the *Department of the Treasury Critical Infrastructure Protection Plan* (CIPP), dated November 1998; the *National Plan for Information Systems Protection,* dated January 2000; and the government-wide Critical Infrastructure Assurance Office's guide entitled, *Practices for Securing Critical Information Assets,* dated January 2000. The review was conducted in the National Office between December 1999 and April 2000. This audit was performed in accordance with *Government Auditing Standards*.

Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Government officials are increasingly concerned about attacks from individuals and groups with malicious intentions, such as terrorists and nations engaging in information warfare.

PDD 63 calls for a national effort to assure the security of the nation's critical infrastructure. The critical infrastructure consists of physical and computer-based systems essential to the minimum operations of the economy and government. The critical infrastructure includes, but is not limited to, telecommunications, banking and finance, energy, transportation, and essential government services.

Advances in information technology have caused the daily activities of our nation's government operations and private businesses to become increasingly automated and inter-linked and have created new vulnerabilities to equipment failures, human error, weather, and physical and computer attacks.[1] The President intends that the United States take all necessary measures to swiftly eliminate any significant vulnerability to both physical and computer attacks on our nation's critical infrastructure, especially our computer systems.

PDD 63 requires that each government department and agency prepare a plan for protecting its own critical infrastructure, including inventorying its mission essential assets, along with analyzing and reducing vulnerabilities.

Results

The IRS has made significant improvements to its overall information security program.

During the last three years, the IRS has devoted significant efforts to improving the overall security of its information systems and facilities. These efforts included: establishing a centralized management function to provide IRS-wide oversight of security controls, implementing new controls designed to

[1] Computer attacks may be defined as the unauthorized electronic access, manipulation, or destruction of electronic data that is being processed, stored, or transmitted on electronic media, resulting in actual or potential harm to the nation's critical infrastructure.

improve the security environment, and conducting numerous on-site evaluations of security at IRS facilities throughout the country. The IRS should be able to use the results of these reviews to help comply with PDD 63. But, to date, this directive has not received sufficient attention.

The Internal Revenue Service Has Taken Limited Actions to Address Critical Infrastructure Planning and Assessment Requirements

Due to other priorities, PDD 63 has not received the necessary attention. As a result, the IRS is in jeopardy of missing the first milestones required by the directive. The December 2000 milestones are critical for the IRS to ensure that the vulnerabilities of its critical infrastructure are known and that plans can be developed to reduce them. Otherwise, the IRS and other agencies and states that use its data could be at undue risk of disrupted operations and processing delays. Until mission essential assets are defined and steps are taken to ensure that each of these assets has been adequately evaluated, IRS management will not have a complete accounting of the vulnerabilities of its critical infrastructure or a clear picture of the actions necessary to comply with PDD 63.

As an individual bureau within the Department of the Treasury, the IRS is not specifically required to prepare a critical infrastructure protection plan. Instead, the Treasury Department issued an initial department-wide plan on November 18, 1998. The IRS has been participating in Treasury-wide working group sessions, which are intended to establish a consistent approach to comply with PDD 63. However, the IRS was awaiting the completion of these efforts by the Treasury Department before taking substantive steps. The IRS recently began taking action to comply with the Treasury CIPP and PDD 63. IRS management

appointed a CIAO in December 1999 and has assigned a limited staff for support.

However, to date, the IRS has not:

- Adequately defined and inventoried mission essential assets associated with critical infrastructure protection.
- Ensured that complete vulnerability assessments for all mission essential assets have been performed.
- Developed a multi-year funding plan for reducing vulnerabilities and a reporting mechanism to track progress in its critical infrastructure protection efforts.

The IRS has not adequately defined and inventoried mission essential assets associated with critical infrastructure protection

IRS management has not defined and inventoried mission essential assets associated with critical infrastructure protection.

PDD 63 requires agencies to define and inventory their assets that are critical to the operations of government. The November 1998 Treasury CIPP provides direction for the bureaus to use in inventorying all of their information systems. Treasury departmental offices and all bureaus were to determine those systems, persons, functions, and facilities which, if lost through destruction or incapacitation, would have a debilitating effect on the Treasury Department's ability to accomplish its national and economic security functions and other essential government services. The Treasury Department's approach was corroborated by the government-wide Chief Infrastructure Assurance Office in *The Practices for Securing Critical Information Assets,* dated January 2000.

For the November 1998 Treasury CIPP, the IRS submitted a list of systems it considered to be critical based on the IRS mission. This list was based on its Year 2000 conversion efforts. The Treasury Department's narrower definition regarding national and economic security and essential government services was not applied in preparing this list. To date, a list of systems meeting the Treasury Department's definition

has not been prepared, nor has the IRS prepared a list of mission essential persons, functions, facilities, and interdependencies.

The IRS has not ensured that complete vulnerability assessments for all mission essential assets have been performed

PDD 63, the *National Plan for Information Systems Protection*, and the Treasury CIPP each require agencies to conduct vulnerability assessments of their assets that are critical to the operations of government. Agencies then must develop plans to improve the vulnerabilities identified.

The IRS has not ensured that complete vulnerability assessments for all mission essential assets have been performed.

During the previous three years, the IRS has conducted vulnerability assessments of IRS facilities and some systems throughout the country. The results of these assessments were cataloged and used to develop corrective action plans for improvement and for the purpose of conducting follow-up assessments. Through these actions, the IRS has made significant progress in improving its security.

It is likely that these reviews have covered many mission essential systems. In this regard, they focused on physical security and access controls over some systems. These reviews may not have included controls for all mission essential computer applications, along with the availability of data and personnel necessary to continue specific critical infrastructure operations. Management cannot be sure that their facility-based efforts have adequately addressed all mission essential assets until the specific assets are identified and their vulnerabilities are assessed.

The IRS also relies on private sector vendors and other agencies to help carry out activities that may be considered mission essential. Management will need to ensure the vulnerabilities associated with these interdependencies are adequately evaluated.

The IRS has indicated that it plans to use disaster recovery and business resumption plans to help reduce the vulnerabilities associated with its mission essential

assets. The current usefulness of these plans is questionable. In our report entitled, *The Internal Revenue Service Needs to Complete Disaster Recovery and Business Resumption Plans,* (Reference Number 2000-20-031, dated March 2000), we noted that the IRS had not completed both disaster recovery and business resumption plans at 30 of 45 major sites. We reviewed plans at five sites and found that these plans did not have all necessary information and did not cover all the important information systems and resources.

The IRS has not developed a multi-year funding plan for reducing vulnerabilities and a reporting mechanism to track progress in its critical infrastructure protection efforts

IRS management has not developed a multi-year funding plan for reducing vulnerabilities and a reporting mechanism to track progress in its critical infrastructure protection efforts.

PDD 63 requires agencies to prepare a multi-year spending plan to enhance controls over the critical infrastructure. The *National Plan for Information Systems Protection* also indicates that, although not required, agency performance measures should include information security. The plan recommends that federal agencies include Government Performance and Results Act of 1993 (GPRA)[2] performance measures to track progress on reducing infrastructure vulnerabilities.

Because it only recently initiated actions to comply with PDD 63, the IRS has not developed a multi-year funding plan for correcting vulnerabilities. Actions to correct deficiencies identified in the ongoing IRS facility-based reviews are currently being funded through various sources, including management at the facility, and by individual program managers through their normal budget process.

Management does not have an overall plan or coordinated method for tracking the funding and budgeting for security improvements, particularly for the critical infrastructure. Also, the IRS has not included PDD 63 efforts in its GPRA performance measures.

[2] Government Performance and Results Act of 1993 (GPRA), Pub. L. No. 103-62, 107 Stat. 285

Congressional interest and oversight of critical infrastructure protection may intensify.

We believe funding for critical infrastructure protection will receive increased oversight from the Congress. The Office of Management and Budget (OMB) may also increase agency reporting requirements. Similar to reactions to the threat of problems from the Year 2000 conversion effort, the possibility for such increased interest in computer security has been demonstrated in the recent OMB Memorandum 00-07, which provides instructions for adequately addressing funding for security controls in Fiscal Year 2002 budget requests.

Also, as the General Accounting Office noted in its report entitled, *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (Reference number GAO/AIMD-00-1, dated October 1999), the Chairman of the President's Council on Year 2000 Conversion stated that agencies should be able to include sufficient funding for information security in their budgets because security improvements and critical infrastructure protection efforts will be ongoing projects. The Chairman of the federal Chief Information Officer's Council Subcommittee on Critical Infrastructure Protection stated that agencies would have serious problems implementing PDD 63 without supplemental funding similar to that provided to help resolve the Year 2000 problem.

Recommendations

1. The CIAO should coordinate with the IRS Chief Information Officer (CIO), IRS functional managers, and senior Department of the Treasury officials to expedite the definition and identification of mission essential assets, including systems, applications, personnel, and data. To expedite these efforts, the CIAO should use the results of the IRS' Office of Security and Privacy Oversight's ongoing efforts to identify and correct security weaknesses associated with these assets.
2. The CIAO should ensure that vulnerabilities to all mission essential assets, including facilities, systems,

applications, personnel, and data, are assessed during future security reviews. In addition, the CIAO should evaluate the interdependencies inherent in the IRS' mission essential activities.

3. The CIAO should develop a multi-year funding plan for reducing the vulnerabilities to mission essential assets.

4. The CIO should incorporate results of PDD 63 efforts with security issues currently being tracked in strategic planning and performance measurement reports for GPRA.

Management's Response: We issued a draft of this report to IRS management on April 28, 2000, with a May 30, 2000, response period. However, management's response was not available as of the date this report was released.

Conclusion

Effective and timely completion of the actions required by PDD 63 is important in ensuring an adequate level of security over the government's infrastructure. As the government's primary revenue collector, the IRS needs to ensure that the risk of disrupted operations and processing delays is kept to a minimum. The IRS has taken steps to improve its overall security program in recent years. However, more emphasis is needed to specifically identify and reduce the vulnerabilities of its mission essential assets.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this review was to evaluate the adequacy of the Internal Revenue Service's (IRS) planning and assessment activities for protecting its critical computer-based infrastructure. To accomplish this, we interviewed management officials and reviewed documentation from recent and ongoing audit projects to evaluate the following aspects of the IRS actions to implement a critical infrastructure protection program.

I. Critical Infrastructure Planning

To determine whether the IRS developed an effective plan for protecting its critical computer-based infrastructure, we:

A. Determined whether the IRS was required to complete a Critical Infrastructure Protection Plan.

B. Determined whether the IRS had appointed a Chief Infrastructure Assurance Officer with overall responsibility for protecting the agency's critical infrastructure.

II. Identification of Critical Assets

To determine whether the IRS has identified its computer-based mission essential assets, we:

A. Determined whether the IRS has identified the following mission essential assets[1] consistent with the criteria used by the government-wide Chief Infrastructure Assurance Office:

1. People (Staff, management - - including security management and executives necessary to plan, organize, acquire, deliver, support, and monitor mission-related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission.)

2. Technology (All hardware and software, connectivity, countermeasures, and/or safeguards that are used in support of the core process.)

[1] The Chief Infrastructure Assurance Office has defined agency mission essential assets 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."

3. Applications (All application systems, internal and external, used in support of the core process.)

4. Data (All data - - electronic and hard copy - - and information required to support the core process. This includes numbers, characters, images, or other methods of recording, in a form which can be assessed by a human or input into a computer, stored and processed there, or transmitted on some digital/communications channel.)

5. Facilities (All facilities required to support the core processes, including the resources to house and support information technology resources.)

B. Evaluated the adequacy of the IRS' efforts to identify mission essential assets and mission essential assets' interdependencies with applicable Federal agencies, state and local government activities, and industry. We determined whether:

1. The IRS used the results of its Year 2000 conversion work in identifying mission essential assets.

2. The asset identification process included a determination of its estimated replacement costs, planned life cycle, and potential impact to the agency if the asset is rendered unusable.

III. Vulnerability Assessments

To assess whether the IRS has adequately (1) identified the threats, vulnerabilities, and potential magnitude of harm to its computer-based mission essential assets that may result from the loss, alteration, unavailability, misuse, or unauthorized access to or modification of its critical computer-based infrastructure investments and (2) developed remediation plans to address the risks identified, we:

A. Determined whether the IRS delegated responsibility for vulnerability assessments to the agency Chief Information Officer.

B. Determined whether the IRS performed and documented an initial vulnerability assessment and developed remediation plans for its mission essential assets.

C. Determined whether the IRS evaluated the level of protection currently in place for its mission essential assets.

D. Determined whether the IRS identified the actions that must be taken before it can achieve a reasonable level of protection for its mission essential assets.

E. Determined whether the IRS developed a related implementation plan and mechanism to monitor such implementation.

F. Determined whether the IRS assessed the vulnerability of its mission essential assets to failures that could result from interdependencies with applicable federal agencies, state and local government activities, and private sector providers of telecommunications, electrical power, and other infrastructure services.

G. Determined whether the IRS adopted a multi-year funding plan that addresses the identified threats.

H. Determined whether the IRS reflected the cost of implementing a multi-year vulnerability remediation plan in its Fiscal Year 2001 budget submission to the Office of Management and Budget.

I. Determined whether the IRS has incorporated its critical infrastructure protection functions into its strategic planning and performance measurement framework.

Appendix II

Major Contributors to This Report

Scott E. Wilson, Associate Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
James T. Avery, Acting Audit Manager
Lawrence R. Smith, Senior Auditor
Billy S. Benge, Auditor
Carol A. Rowland, Auditor

Appendix III

Report Distribution List

Chief Information Officer IS
Director, Office of Security and Privacy Oversight IS:SPO
Director, Security, Evaluation and Oversight IS:SPO:S
Director, Office of Program Evaluation and Risk Analysis M:O
National Director for Legislative Affairs CL:LA
Office of Chief Counsel CC
Office of the National Taxpayer Advocate C:TA
Office of Management Controls M:CFO:A:M
Audit Liaison:
Chief Information Officer IS