

**Letter Report: Planning Efforts to Protect
Critical Infrastructure Facilities Are Adequate**

July 2001

Reference Number: 2001-20-111

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

July 24, 2001

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

A handwritten signature in cursive script that reads "Pamela J. Gardiner".

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Letter Report - Planning Efforts to Protect Critical
Infrastructure Facilities Are Adequate

This report presents the results of our review of the Internal Revenue Service's (IRS) compliance with Federal critical infrastructure policies. In summary, we found the IRS has made progress to support the physical security goals of Presidential Decision Directive 63, which calls for a national effort to ensure the security of the nation's critical infrastructure. The IRS has identified its critical infrastructure facilities, conducted vulnerability assessments, and determined what corrective actions are needed. Management agreed with the information presented in this report, and the full text of their response is included as an appendix.

Copies of this report are being sent to the IRS managers who are affected by the report and to the President's Council on Integrity and Efficiency. Please contact me at (202) 622-6510 if you have questions or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

Letter Report: Planning Efforts to Protect Critical Infrastructure Facilities Are Adequate

Objective and Scope

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

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 infrastructure facilities, as required by Presidential Decision Directive (PDD) 63. We conducted this review in conjunction with other similar audits being performed by other Inspector General offices, as directed by the President's Council on Integrity and Efficiency (PCIE).¹ We issued an earlier report² which addressed the planning and assessment activities of computer-based assets pertaining to the IRS' critical infrastructure.

To accomplish our objective, we determined whether vulnerabilities and actions to reduce the vulnerabilities had been identified. We also determined whether the planned actions had been funded. We interviewed the Chief Infrastructure Assurance Officer (CIAO) and personnel in the Special Projects branch of the Office of Security. We reviewed the IRS' draft Critical Infrastructure Plan and all vulnerability assessments and security/risk reviews of its critical infrastructure facilities conducted within the last 4 years. We performed our audit work between January and April 2001 in the National Headquarters.

This audit was performed in accordance with *Government Auditing Standards*. Major contributors to this report are listed in Appendix I. Appendix II contains the Report Distribution List.

¹ The PCIE consists of representatives from Inspector General offices.

² *The Internal Revenue Service Should Improve Actions to Protect Its Critical Infrastructure* (Reference Number 2000-20-097, dated June 2000).

Letter Report: Planning Efforts to Protect Critical Infrastructure Facilities Are Adequate

Background

PDD 63, signed in May 1998, called for a national effort to assure the security of the nation's critical infrastructure.

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, signed in May 1998, called for a national effort to ensure the security of the nation's critical infrastructure. The critical infrastructure is defined as 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, and transportation.

In response to PDD 63, the Department of the Treasury completed a Critical Infrastructure Protection Plan (CIPP) as a guide for all of its offices and bureaus. The CIPP requires that all Department of the Treasury offices and bureaus appoint a CIAO who has overall responsibility for protecting his/her organization's critical infrastructure.

The IRS appointed the Director, Office of Security, as the CIAO. The responsibilities of the CIAO include: identifying all critical infrastructure facilities, determining the appropriate level of security for the facilities, identifying existing vulnerabilities at the facilities, and remedying the vulnerabilities to ensure the appropriate level of security.

Results

The IRS identified its critical infrastructure facilities, conducted vulnerability assessments, and determined what corrective actions are needed.

The IRS has made progress to support the physical security goals of PDD 63. The CIAO identified the IRS' critical infrastructure facilities and determined the appropriate level of security needed to adequately protect the facilities. The Office of Security conducted vulnerability assessments of the facilities and identified several actions that must be taken to meet the level of security recommended by the CIAO. Some of the

Letter Report: Planning Efforts to Protect Critical Infrastructure Facilities Are Adequate

security enhancements recommended include physical upgrades to improve the effectiveness of:

- Property and building access controls.
- Guard force capabilities.
- Surveillance and alarm capabilities.

Though corrective actions have not been started, the CIAO has initiated activities to fund these actions.

As of April 2001, none of the actions identified in the vulnerability assessments had been started and the CIAO could not provide a definitive time period when they will be completed. However, the CIAO has initiated actions to obtain funding for the security upgrades.

The CIAO discussed the proposed level of security with the Financial and Management Controls Executive Steering Committee, which is chaired by the IRS Deputy Commissioner, in March 2001. The Committee approved the level of security proposed by the CIAO.

The upgrades needed to reach that level of security are estimated to cost over \$8 million. The CIAO is attempting to obtain funding for the upgrades in Fiscal Year 2001. If funding is not available this fiscal year, the CIAO intends to include the funding for the upgrades in the Fiscal Year 2002 budget.

If funding is not provided to adequately protect the IRS' critical infrastructure facilities, 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.

Conclusion

The IRS has taken steps to identify its critical infrastructure facilities, assess the vulnerabilities of the facilities, and identify corrective actions. The CIAO has initiated steps to fund these actions. IRS management agreed with the information in this report, and the full text of their response is included as Appendix III.

**Letter Report: Planning Efforts to Protect Critical
Infrastructure Facilities Are Adequate**

Appendix I

Major Contributors to This Report

Scott Wilson, Assistant Inspector General for Audit (Information Systems Programs)

Steve Mullins, Director

Kent Sagara, Audit Manager

Bill Lessa, Senior Auditor

David Hodge, Auditor

**Letter Report: Planning Efforts to Protect Critical
Infrastructure Facilities Are Adequate**

Appendix II

Report Distribution List

Commissioner N:C

Deputy Commissioner N:DC

National Taxpayer Advocate TA

Chief Counsel CC

Director, Office of Security M:S

Director, Legislative Affairs CL:LA

Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O

Office of Management Controls N:CFO:F:M

President's Council on Integrity and Efficiency

Audit Liaison:

Deputy Commissioner for Modernization & Chief Information Officer M

**Letter Report: Planning Efforts to Protect Critical
Infrastructure Facilities Are Adequate**

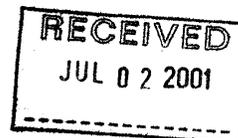
Appendix III

Management's Response to the Draft Report



DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224



June 29, 2001

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:


John C. Reece
Deputy Commissioner for Modernization &
Chief Information Officer

SUBJECT:

Draft Letter Report – Planning Efforts to Protect Critical
Infrastructure Facilities are Adequate

Thank you for the opportunity to review and comment on your draft report, of the IRS' Critical Infrastructure Protection (CIP) efforts to protect critical facilities.

Security at the IRS has been a top priority for the agency for the past four years. The Service's aggressive security management program has been focused on identifying, managing, and mitigating security weaknesses. To date, it has resulted in measurable improvements with a significant number of security enhancements being implemented in response to earlier vulnerability assessments. These have included major upgrades to the IRS' critical facilities. As noted in your draft report, the IRS is actively engaged in more recent efforts to further enhance security at these facilities. These efforts have also identified the need for resources to upgrade security at the facilities.

As with any entity, the resources for unanticipated needs—such as these security upgrades—are not readily available. Current efforts to obtain funds include a risk-based prioritization of the enhancements for each facility, so that the IRS can phase in the security upgrades as it identifies additional funding sources. I believe that the Service's efforts and approach provide a process that allows it to effectively manage this area.

If you would like to discuss my response in more detail, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Director, Office of Security at (202) 622-8910.