



Audit Report



OIG-07-045

INFORMATION TECHNOLOGY: BEP Improved Controls Over Its Computer Security Incidence Response Capability (Corrective Action Verification on OIG-05-039)

September 11, 2007

Office of
Inspector General

Department of the Treasury

Contents

Audit Report

Background	3
Objective, Scope, and Methodology.....	4
Corrective Actions Taken by BEP	5

Appendices

Appendix 1: Management Response	8
Appendix 2: Report Distribution.....	9

Abbreviations

BEP	Bureau of Engraving and Printing
CAV	Corrective Action Verification
CSIRC	Computer Security Incident Response Capability
IDS	Intrusion Detection System
IT	Information Technology
JAMES	Joint Audit Management Enterprise System
OCIITS	Office of Critical Infrastructure and Information Technology
POA&M	Plan of Action and Milestone
TCSIRC	Treasury Computer Security Incident Response Center
TD P	Treasury Directive Publication

This page intentionally left blank.

*The Department of the Treasury
Office of Inspector General*

September 11, 2007

Larry R. Felix
Director
Bureau of Engraving and Printing

This report presents the results of our review of corrective actions taken by the Bureau of Engraving and Printing (BEP) in response to the four recommendations we made in our June 2005 report on the BEP's Computer Security Incident Response Capability (CSIRC).¹ These recommendations involve updating the CSIRC policy and procedures; establishment of an intrusion detection system; and reporting computer security incidents to Treasury's Computer Security Incident Response Center (TCSIRC). According to the record in Treasury's Joint Audit Management Enterprise System (JAMES), BEP closed the four recommendations by early May 2006, indicating that it had completed corrective action in response to the recommendations.

We found that BEP took appropriate corrective actions that met the intent of our prior recommendations.

Background

According to Office of Management and Budget Circular A-50, audit follow-up is an integral part of good management and a shared responsibility of management and auditors.² Each agency, the circular states, should establish an audit follow-up system to assure the prompt and proper resolution and implementation of audit recommendations. Treasury Directive (TD) 40-03 requires bureau staff to ensure that (1) audit recommendations are resolved

¹ *BEP's Computer Security Incident Response Capability Needs Improvement*, OIG-05-039 (June 30, 2005)

² OMB Circular A-50, revised, *Audit Followup* (September 29, 1982)

on a timely basis; (2) resolved audit recommendations (i.e., those agreed to by bureau management) are promptly acted upon and that progress with respect to proposed and ongoing corrective actions is adequately monitored; and (3) statistical information and other data are appropriately reported pursuant to all statutory and regulatory requirements.³

At the departmental level, the status of audit recommendations is tracked in JAMES, an interactive system accessible to both the Treasury Office of Inspector General and bureau management. JAMES contains tracking information on audit reports from their issuance through completion of all actions related to the findings and recommendations they contain. At the bureau level, BEP uses its own internal tracking system along with JAMES. In addition, information technology related issues are tracked in the agency's plans of actions and milestones (POA&M) and the related information is recorded in the internal tracking system. During 2007, Treasury expected bureaus to update outstanding POA&Ms into the Treasury's Trusted Agent FISMA system (TAF).

BEP's Office of Compliance coordinates the development of BEP responses to audit findings and recommendations. The Chief of Office of Compliance validates the planned corrective actions developed by responsible program officials, and its staff record, monitor, and track implementation of the planned corrective actions in the internal tracking system. For information technology related audit recommendations, BEP's Office of Critical Infrastructure & IT Security (OCIITS) is responsible for the development and implementation of planned corrective actions.

Objective, Scope, and Methodology

The objective of this CAV was to determine whether BEP management had taken corrective actions responsive to the intent of our recommendations to improve controls and oversight over the BEP's CSIRC. This CAV addresses the planned corrective actions associated with the recommendations in our June 2005 report on the BEP's CSIRC.

³ Treasury Directive 40-03, *Treasury Audit Resolution, Follow-Up, and Closure* (February 2, 2005).

We met with the chief and staff from the Office of Compliance as well as the chief and staff of OCIITS to obtain an understanding of the process used to monitor the status of recommendations recorded in JAMES and TAF. We reviewed the BEP's updated manuals and reports relating to CSIRC. We obtained supporting documents to review the policy implementation and compliance in more detail. We queried JAMES to review the status of the recommendations.

We conducted our audit from March 2007 to June 2007 at BEP headquarters in Washington, D.C., in accordance with generally accepted government auditing standards.

Corrective Actions Taken by BEP

Prior Recommendation 1. Ensure that current BEP CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01, *Treasury IT Security Program*.

In response to this recommendation, BEP updated and reissued its CSIRC manual in November 2005. The updated CSIRC manual incorporated the guidance established by TD P 85-01. We believe that BEP addressed the intent of our recommendation.

Prior Recommendation 2. Ensure BEP's *Security Awareness and Training Policy* is updated and incorporates the guidance established by TD P 85-01.

In response to this recommendation, BEP included TD P 85-01 as a reference in its *Security Awareness and Training Policy*. The updated training policy correctly references to the guidance established by TD P 85-01. We believe that BEP addressed the intent of our recommendation.

Prior Recommendation 3. Ensure that an Intrusion Detection System (IDS) is established for BEP's computer operations to ensure that computer security incidents are being accurately identified and reported.

BEP completed the planned corrective action for this recommendation – implementation of an IDS – and closed the recommendation in JAMES on May 5, 2006. Shortly after its implementation, BEP found that the IDS overloaded the network and significantly slowed down network trafficking. Subsequently, BEP immediately deactivated the IDS and opened a POA&M to track resolution of the problem in TAF.

After conducting more tests, the IDS was re-implemented, and the POA&M was closed in TAF in early May 2007. Consequently, we believe that BEP addressed the intent of our recommendation.

Prior Recommendation 4. Ensure that computer security incident information is consistently reported to TCSIRC by the fifth calendar day of each month.

We reviewed monthly CSIRC reports submitted from June 2006 through April 2007 and found that BEP submitted the Treasury-required monthly reports to TCSIRC in time for each month. Consequently, we believe that BEP addressed the intent of our recommendation.

Management Response

In a memorandum dated September 7, 2007 (Appendix 1), the BEP associate director concurred with our draft report and reaffirmed the BEP's commitment to establishing and maintaining effective internal control in its operations.

* * * * *

We would like to extend our appreciation for the cooperation and courtesies extended to our staff during the review. If you have any questions, please contact me at (202) 927-5746. The major contributor to this report was Myung Han, Management Analyst.


Cedric E. Hammond, Sr.
Acting Director, Fiscal Service Audits



DEPARTMENT OF THE TREASURY
BUREAU OF ENGRAVING AND PRINTING
WASHINGTON, D.C. 20228

September 7, 2007

MEMORANDUM FOR CEDRIC E. HAMMONDS, SR.
ACTING DIRECTOR, FISCAL SERVICE AUDITS
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY

FROM: 
Leonard R. Olfar
Associate Director
Chief Financial Officer

SUBJECT: Formal Draft Audit Report "Information Technology: BEP
Improved Controls Over Its Computer Security Incidence
Response Capability (Corrective Action Verification on
OIG-05-039)."

The Bureau of Engraving and Printing has reviewed the Treasury Department Office of the Inspector General's (OIG) formal audit report, "Information Technology: BEP Improved Controls Over Its Computer Security Incidence Response Capability (Corrective Action Verification on OIG-05-039)."

We are pleased that the corrective actions taken by the Bureau of Engraving and Printing have been validated by your office and found to be appropriate in correcting the previously reported conditions. The Bureau of Engraving and Printing is committed to establishing and maintaining effective internal controls to prevent fraud, waste, abuse and mismanagement in our operations, and this corrective action verification audit afforded us the opportunity to confirm our efforts to resolve noted weaknesses.

Department of the Treasury

Deputy Chief Financial Officer
Office of Performance Budgeting and Strategic Planning
Office of Accounting and Internal Control

Bureau of Engraving and Printing

Director
Audit Liaison Official

Office of Management and Budget

OIG Budget Examiner