



Audit Report



OIG-05-039

BEP's Computer Security Incident Response

Capability Needs Improvement

June 30, 2005

Office of
Inspector General

Department of the Treasury

Contents

Audit Report	3
Results In Brief.....	4
Background	4
Findings and Recommendations	6
BEP’s CSIRC Policy And Procedures Need To Be Updated.....	6
Recommendations.....	8
BEP’s Computer Security Incident Reporting Was Not Complete	9
Recommendations.....	11

Appendices

Appendix 1: Objective, Scope, and Methodology	13
Appendix 2: Overview of Treasury’s CSIRC Structure	14
Appendix 3: BEP CSIRC Procedures Comparison With TD P 85-01	16
Appendix 4: Management Comments	19
Appendix 5: Major Contributors.....	21
Appendix 6: Report Distribution.....	22

Tables

Table 1: Computer Security Incidents	16
Table 2: Comparison of Treasury Incident Response Procedures with BEP Procedures	17

Abbreviations

BEP	Bureau of Engraving and Printing
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
FISMA	Federal Information Security Management Act
FY	Fiscal Year
IDS	Intrusion Detection System
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

Contents

OMB	Office of Management and Budget
TCSIRC	Treasury's Computer Security Incident Response Center
TD P	Treasury Directive Publication
Treasury	Department of the Treasury

*The Department of the Treasury
Office of Inspector General*

June 30, 2005

Ronald W. Falter
Chief Information Officer
Bureau of Engraving and Printing

The Office of Inspector General's (OIG) Annual Plan for Fiscal Year (FY) 2004 included the audit project, *Independent Evaluation of Treasury's Information Security Program and Practices Pursuant to the Federal Information Security Management Act (FISMA)*. As part of this review, the OIG was required to evaluate aspects of the Department of the Treasury's (Treasury) computer security incident response capability (CSIRC). During our FY 2003 FISMA independent evaluation, we noted that the number of computer security incidents reported by Treasury bureaus varied significantly. The Office of Management and Budget (OMB) reported similar divergence in incident numbers reported across Federal agencies in its FY 2003 FISMA report to Congress in March 2004.

This audit was structured based on current, as well as prior, OMB FISMA reporting requirements. The OIG plans to incorporate the results of this audit into its FY 2005 FISMA evaluation. This audit is also consistent with Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology Security Program*¹, which requires that Treasury bureaus establish and maintain an incident response capability.

Our overall objective for this audit was to determine if the Bureau of Engraving and Printing (BEP) established an adequate CSIRC process. To accomplish this objective, we: (1) interviewed BEP information technology (IT) personnel; (2) reviewed relevant IT policy and procedure documents; and (3) observed the actual IT reporting processes that produce CSIRC and software patch management data. A more detailed description of our objective, scope, and methodology is provided in Appendix 1.

¹ *Treasury IT Security Program* (TD P 85-01) was updated as of August 15, 2003.

Results In Brief

Overall, we found that although BEP established a CSIRC and a software patch management function, its computer security incident reporting process needs improvement. For instance, we identified that BEP: (1) CSIRC, security awareness, and training policy and procedures were based on outdated Treasury policy; (2) CSIRC procedures did not incorporate all required aspects of Treasury's current IT security policy; (3) did not establish an intrusion detection system (IDS); and (4) needs to ensure the timely reporting of computer security incidents to Treasury's Computer Security Incident Response Center (TCSIRC).

Our report includes several recommendations that, in our opinion, will assist BEP in remedying the deficiencies identified above. Specifically, we are recommending that BEP's Chief Information Officer (CIO) ensure that:

1. Current BEP CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01.
2. BEP's *Security Awareness and Training Policy* is updated and incorporates the guidance established by TD P 85-01.
3. An IDS is established for BEP's computer operations to ensure that computer security incidents are being accurately identified and reported.
4. Computer security incident information is consistently reported to TCSIRC by the fifth calendar day of each month.

Background

According to the National Institute of Standards and Technology (NIST), computer security incident response has become an important component of IT programs.² Security-related threats have become not only more numerous and diverse, but also more damaging and disruptive. New types of security-related incidents emerge frequently. Preventative activities based on the results of risk assessments can lower the number of incidents, but not all incidents can be prevented. An incident response capability is

² NIST Special Publication 800-61, "*Computer Security Incident Handling Guide*", dated January 2004.

therefore necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services.

NIST guidance also states that since performing incident response effectively is a complex undertaking, establishing a successful incident response capability requires substantial planning and resources.³ Continually monitoring threats through an IDS is essential. Establishing clear procedures for assessing the current and potential business impact of incidents is critical, as is implementing effective methods of collecting, analyzing, and reporting data. Building relationships and establishing suitable means of communication with other internal groups (e.g., human resources, legal) and with external groups (e.g., other incident response teams, law enforcement) are also vital.

TCSIRC provides a means for receiving and/or disseminating computer security incident information to Treasury bureaus; and consistently responding to, and reporting on, computer security incidents. See Appendix 2 for an overview of the TCSIRC structure and functionality.

BEP's CSIRC has primary jurisdiction over incident response activities for all BEP information systems, including those administered by the CIO or other directorate, or their contractors. Also, BEP's CSIRC offers incident prevention, detection, response, and reporting services, such as:

- Disseminating applicable bulletins and advisories.
- Administering software security updates.
- Risk mitigation tracking and reporting.
- Anti-virus protection.
- IT security training.

In addition, BEP's CSIRC policy and procedures apply to all persons who use or administer BEP information technology resources.

³ NIST Special Publication 800-61, *"Computer Security Incident Handling Guide"*, dated January 2004.

Findings and Recommendations

Although deficiencies existed in its current CSIRC process, we identified areas where BEP was taking appropriate steps in establishing an adequate CSIRC and software patch management function. For example:

- BEP established a CSIRC function operated by the Office of Critical Infrastructure and IT Security.
- A software patch management system was established for the distribution and application of patches. In addition, a patch testing lab was established where patches are tested prior to being uploaded onto BEP's network.
- BEP established patch management procedures identifying a systematic approach for identifying and installing necessary security patches.⁴
- An Anti-Virus Operations Handbook was being drafted that will provide comprehensive procedures required to implement the BEP anti-virus program and document the activities related to anti-virus protection of e-mail and network resources.
- BEP established an IT security awareness training program for both IT users and non-IT users. The program addresses topics such as risk management, risk assessment, virus prevention, password protection, and incident response.

Finding 1 BEP's CSIRC Policy And Procedures Need To Be Updated

BEP's policies and procedures relating to CSIRC were not current with Treasury guidance. More specifically: (1) CSIRC, security awareness, and training policy and procedures were based on outdated Treasury policy; and (2) CSIRC procedures did not incorporate all required aspects of Treasury's current IT security policy. By not updating current policies and procedures, BEP cannot ensure that IT security personnel will address computer security incidents appropriately.

⁴ *Patch Management, Bureau of Engraving and Printing*, dated April 13, 2004.

BEP's CSIRC Policy Is Not Based On Current Treasury Policy

We found that although BEP established a policy regarding its CSIRC process, this policy was not based on current Treasury policy. BEP's current policy⁵ was designed to ensure compliance with all laws and regulations relating to the identification, reporting, and response to computer and network security breaches, viruses, and web attacks. However, this policy is based on Treasury Security Manual TD P 71-10. In August 2004, the Treasury CIO issued a memorandum stating that Treasury had updated its IT security policy and that TD P 85-01 now formally documents the IT security program. As a result, TD P 85-01 superceded TD P 71-10. During the audit, we were informed that BEP's CSIRC policy was being updated to incorporate the requirements of TD P 85-01.

BEP's *Security Awareness And Training Policy* Is Not Based On Current Treasury Policy

Although BEP established a policy⁶ for its information security awareness and training, this policy was not based on current Treasury policy. This policy was designed to ensure that employees and contractors are aware of information security principles, risks to IT systems, understand the roles and responsibilities related to information security, and are appropriately trained to fulfill them. This policy was also based on TD P 71-10. By not incorporating the policy guidance mandated by TD P 85-01, BEP's *Security Awareness And Training Policy* is not current with Treasury's IT security policy.

BEP's CSIRC Procedures Are Not Based On Current Treasury Policy

We also found that BEP established procedures regarding its CSIRC process. BEP's current procedures⁷ identify the resources necessary to prevent, identify, respond to, resolve, and report

⁵ Bureau of Engraving and Printing Circular No. 10-08.22, "*Computer Security Incident Response Capability*", dated May 21, 2001.

⁶ Bureau of Engraving and Printing Circular No. 10-08.28, "*Information Security Awareness and Training Policy*", dated July 31, 2002.

⁷ "*Computer Security Incident Response Capability Manual*", No. 10-08.29, dated July 31, 2002.

computer security incidents that may adversely affect BEP's IT resources and ability to accomplish its mission. However, these procedures were based on TD P 71-10. After comparing current BEP CSIRC procedures with TD P 85-01, we identified the following areas where BEP CSIRC procedures did not incorporate TD P 85-01 requirements:

- Section 2.6 – CSIRC definitions and classifications.
- Section 2.7.6 – Bureau CSIRC responsibilities.
- Section 3.2.1 – Individual (significant) incident reporting.
- Section 3.2.2 – Monthly (minor) incident reporting.
- Section 3.3.1 – Significant incident reporting methods.
- Section 4.1.4 – Eradication process for incident handling.
- Section 4.2.4 – Reporting incidents as closed when resolved.
- Section 4.2.4 – Reporting subsequent incident information to TCSIRC.
- Section 5.1 – Bureau CSIRC distributes advisories and bulletins to appropriate bureau personnel.

Appendix 3 has a detailed listing of the requirements for each of the sections identified above. By not incorporating the policy guidance mandated by TD P 85-01, BEP's CSIRC procedures are not current with Treasury's IT security policy.

Recommendations

The CIO should ensure that:

1. Current BEP CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01.
2. BEP's *Security Awareness and Training Policy* is updated and incorporates the guidance established by TD P 85-01.

Management Response Management agreed with the recommendation, and they have updated their policies to include the provisions and guidance included in TD P 85-01 which were not included in their policies and procedures at the time of our audit.

OIG Comment The actions taken by BEP are responsive to the intent of our recommendations.

Finding 2

BEP's Computer Security Incident Reporting Was Not Complete

BEP did not establish a complete process for reporting its computer security incidents. For instance, BEP did not establish an IDS to ensure that all computer security incidents were detected and reported. In addition, BEP was not reporting its computer security incident information within the required timeframe to TCSIRC. Without a complete security incident reporting process, BEP cannot ensure that computer security incidents are being detected and reported.

BEP Did Not Establish An Intrusion Detection System

We found that BEP did not establish an internal or external IDS for its computer operations. An IDS allows IT security personnel to observe and react to a variety of anomalous behaviors on monitored networks and server machines by creating a continuous log file of substantial event data. Further, an IDS provides a second line of defense that exists beyond a firewall. Without establishing an IDS, BEP cannot ensure that all computer security incidents are being detected and reported. Further, by not employing an IDS, BEP will be understating its computer security incident reporting to TCSIRC, as well as for FISMA reporting.

In addition, we requested to review Help Desk tickets relating to computer security incidents that were generated for May 2004. We found that BEP did not have any Help Desk tickets regarding computer security incidents for May 2004. The lack of security incidents being reported by the Help Desk might have been impacted by the absence of an IDS.

BEP Needs To Ensure Timely Reporting To TCSIRC

TD P 85-01 requires that bureaus submit monthly computer security incident reports to TCSIRC by the fifth calendar day of each month. We reviewed the listing of BEP's monthly computer security incident reports received by TCSIRC for October 2003

through July 2004. Although BEP was reporting its information on a monthly basis to TCSIRC, we found that for two of the months,⁸ TCSIRC did not receive BEP's computer security incident information by the required due date. By not having its computer security incident information to TCSIRC by the required reporting date, BEP is not meeting the reporting requirements of TD P 85-01.

Appendix III to OMB Circular A-130, *Security of Federal Automated Information Resources*, requires that agencies establish, as part of a system security plan, an incident response capability. This capability should ensure that help is provided to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats. This capability shall share information with other organizations consistent with NIST coordination. Appendix III also requires that an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms.

The *Treasury Information Technology Security Program*, TD P 85-01, establishes comprehensive, uniform IT security policies to be followed by each bureau in developing its own specific policies and operating directives. The Treasury IT Security Program serves as a foundation for the bureaus' IT security programs. TD P 85-01 clarifies national policies, adapts them to Treasury's specific circumstances, and imposes additional requirements when necessary.

TD P 85-01 outlines procedures for an incident response capability designed to receive and disseminate incident information and provide a consistent capability to respond to and report on incidents. It also provides guidance to Treasury bureaus, Departmental Offices, the OIG, and the Treasury Inspector General for Tax Administration staff on responding to and reporting security incidents that affect Treasury's ability to conduct its mission. Specifically, TD P 85-01 provides for the following:

⁸ November 2003 and March 2004.

-
- A framework for identifying, handling, managing, responding to, and reporting incidents in a timely and expeditious fashion.
 - A mechanism for disseminating generic and specific incident information to the CIOs and bureaus to ensure that actions are being taken to minimize the impact of ongoing or potential incidents.
 - Government-wide information sharing of threats, incidents, and trends to support security planning and operations.

Without updating its CSIRC policy and procedures, as well as establishing a complete CSIRC process, BEP is not accurately identifying and accounting for all its computer security incidents. As a result of understating its computer security incident reporting, BEP may not be accurately addressing the reporting requirements mandated by FISMA. In addition, by not incorporating the policy guidance mandated by TD P 85-01, BEP's *Security Awareness and Training Policy* will not be current with Treasury's IT security policy.

Recommendations

The CIO should ensure that:

3. An IDS is established for BEP's computer operations to ensure that computer security incidents are being accurately identified and reported.
4. Computer security incident information is consistently reported to TCSIRC by the fifth calendar day of each month.

Management Response Management agreed with the recommendation and is currently evaluating host-based IDS's and will be implementing a system following the comparison, evaluation, and testing of the product. Additionally, management indicated that the late reporting incidents were exception's to BEP's normal reporting process. Management stated that they provided TCS advance notice and TCS concurred with the late reporting.

OIG Comment The actions taken and planned by BEP for Information Systems are responsive to the intent of our recommendations.

* * * * *

I would like to extend my appreciation to BEP for the cooperation and courtesies extended to my staff during the review. If you have any questions, please contact me at (202) 927-5774. Major contributors to this report are listed in Appendix 5.

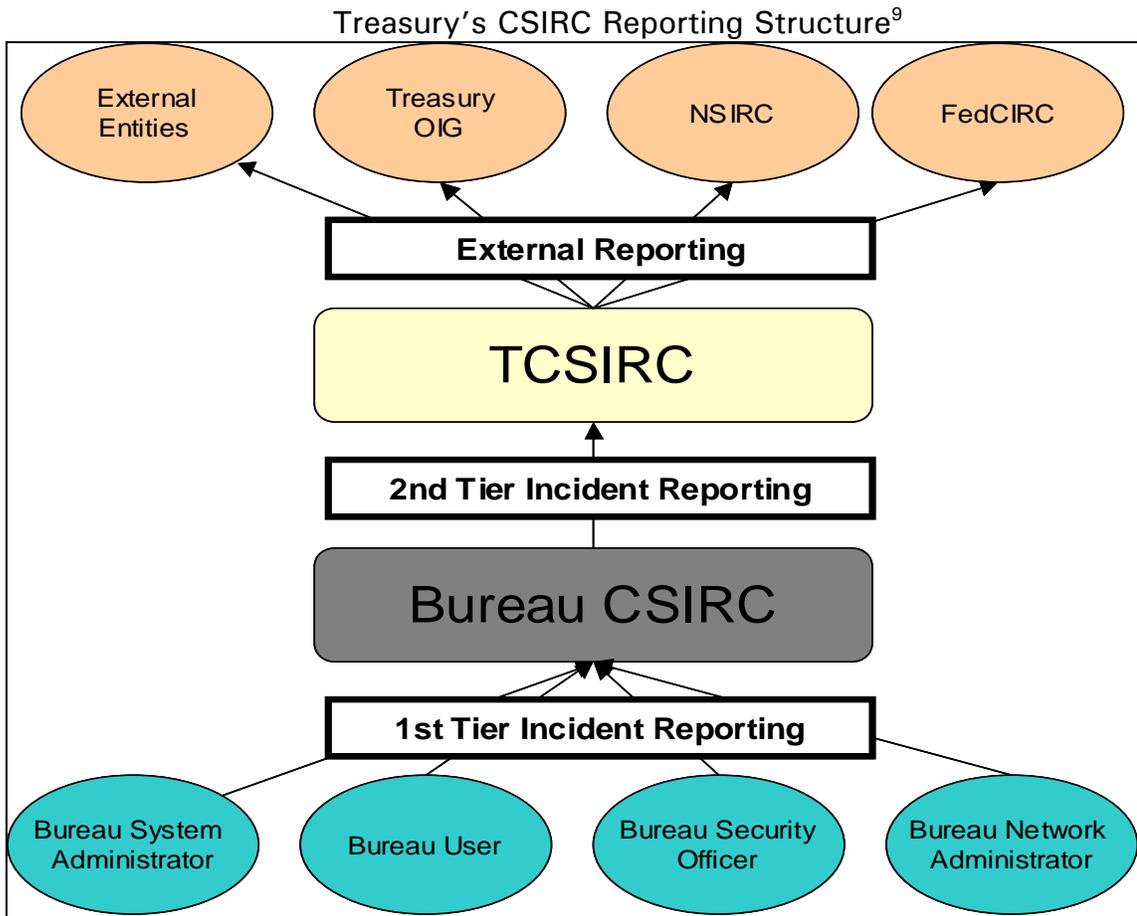
/s/

Louis C. King
Director, Information Technology Audits

The objective of this audit was to determine if BEP established an adequate CSIRC process. This objective was accomplished by determining if BEP established and implemented CSIRC policy and procedures compliant with Treasury and OMB criteria. We performed this audit by: (1) interviewing appropriate Office of Critical Infrastructure and IT Security personnel; (2) obtaining and reviewing applicable CSIRC and software patch management process documentation; (3) obtaining and analyzing bureau level and Departmental level CSIRC data; and (4) observing bureau level and Departmental level CSIRC processes.

Our standards for CSIRC and software patch management performance for this audit were based solely on the bureau requirements published in Treasury Department Publication TD P 85-01 and OMB agency reporting requirements for FY 2003 FISMA.

This report details the fieldwork performed at BEP's headquarters site in Washington, DC, from May through September 2004. We conducted our audit in accordance with generally accepted government auditing standards.



Source: Treasury IT Security Program (TD P 85-01)

The TCSIRC serves as a 24 hours a day, 7 days a week, 365 days a year, escalation center and as the central point of contact for incidents within Treasury. The TCSIRC facilitates incident reporting to the Treasury OIG, and with external reporting entities. In addition, TCSIRC provides the following functions:

- A framework for identifying, handling, managing, responding to, and reporting computer incidents in a timely and expeditious manner.
- A mechanism for disseminating generic and specific computer security incident information to ensure that actions are being taken to minimize the impact of ongoing or potential incidents.

⁹ As of September 2003, the United States Computer Security Readiness Team (US-CERT) replaced FedCIRC in protecting the nation's Internet infrastructure against cyber attacks.

- Government-wide information sharing of threats, incidents, and trends to support computer security planning and operations.

The following table defines computer security incidents that should be reported to TCSIRC.

Table 1: Computer Security Incidents

Incident Type	Incident Description
Malicious Logic Attacks	Performed by crackers/hackers attempting to gain privileges and/or information, capture passwords, and modify audit logs to hide unauthorized activity. Attempts include viruses, Trojan horses, worms, and scripts.
Probes and Reconnaissance Scans	Includes probing or scanning networks for critical services or security weaknesses.
Unauthorized Access and Unsuccessful Attempts	All successful unauthorized accesses and suspicious unsuccessful attempts.
Denial-of-Service Attacks	Affect the availability of critical resources, such as e-mail servers, web servers, routers, gateways, and communication infrastructure.
Alterations/Compromises of Information	Involve the unauthorized altering of information or the compromise of information.
Adverse Site Mission Impacts	Significantly impact the mission of the site or operations.
Classified System Incidents	Involve either a system used to process national security information, or classified information on any system not certified for that level of classified information.
Loss or Theft of Equipment With Classified Information	Includes the compromise of user accounts and passwords allowing unauthorized persons access to Treasury computing resources, agents' names, or case information that could compromise an investigation or risk the loss of human life. Emphasis is on the data that was lost or stolen, not on the hardware itself.
Misuse of Resources	Misuse of a computing or telecommunications system or network by an authorized user.
Domain Name System Attacks	Affect the availability of services or networks.
Root Compromise	Compromise the most trusted privileges of the machines on the network.
Web Site Defacements	Superficial destruction of web pages that could cause embarrassment, but not lead to an attack.

Source: Treasury IT Security Program (TD P 85-01)

As part of our review, we compared the requirements cited in TD P 85-01 with BEP’s current CSIRC procedures. The following table contains requirements cited in TD P 85-01 that were not found in BEP Manual No. 10-08.29.

Table 2: Comparison of Treasury Incident Response Procedures With BEP Procedures

TD P 85-01 Section	Specific Treasury Incident Response Procedures Not Found In BEP’s CSIRC Manual No. 10-08.29
<u>Section 2.6</u> – CSIRC Definitions and Classifications	“Event” Definition: “A notable occurrence, not yet assessed, in a computing or telecommunications system or network that may affect that system or network.”
	“Incident” Definition: “The violation of an explicit or implied security policy in a computing or telecommunications system or network.”
	“Significant Incident” Classifications: Unauthorized alteration or compromise of data; classified incident; denial of service attack; DNS attack; loss or theft of equipment with classified information; successful malicious code infection; root compromise; unauthorized access; website defacement; other.
	“Classified Incident” Definition: “Any event that involves a system used to process national security information, a critical infrastructure protection asset, or any discovery of classified information on any system not certified for that level of classified information.”
<u>Section 2.7.6</u> – Bureau CSIRC Responsibilities	“Provide monthly summary reports of minor incidents to the TCSIRC by the 5 th calendar day of each month for incidents that occurred the previous month.”
<u>Section 3.2.1</u> – Individual (Significant) Incident Reporting	“Upon identification of a significant incident, the bureau CSIRC must provide a preliminary report to the TCSIRC within one hour.”
	“Within four hours of the initial report, the bureau CSIRC must provide a more detailed report.”
	“The bureau CSIRC must update the TCSIRC every four hours until incident resolution occurs.”
	“The bureau CSIRC must update the TCSIRC as new information about the incident is discovered.”
	“The bureau CSIRC must provide the information outlined in the “Incident Report Form” (Appendix C).”
(Table Continued On The Next Page)	

Table 2: Comparison of Treasury Incident Response Procedures With BEP Procedures (Cont.)

TD P 85-01 Section	Specific Treasury Incident Response Procedures Not Found In BEP Manual No. 10-08.29
<p><u>Section 3.2.2</u> – Monthly (Minor) Incident Reporting</p>	<p>“Reports containing classified incidents must be sanitized to avoid unauthorized disclosure.”</p> <p>“Reports containing classified information must be reported through appropriate secure communications.”</p> <p>“Monthly reports from the bureau CSIRC to TCSIRC must contain the following information: the top 5 originating internet protocol addresses that generated the most activity across all minor incidents; misuse of resources; loss or theft of equipment (unclassified); probes or reconnaissance scans; unsuccessful access and penetration; and malicious code detection. Also, any additional information such as feedback on TCSIRC performance, other incidents, and changes in bureau points of contact data.”</p>
<p><u>Section 3.3.1</u> – Significant Incident Reporting Methods</p>	<p>Unclassified systems (electronic mail, fax, telephone, online incident report. Critical infrastructure protection assets (STU/III, secure fax). Classified incidents (STU/III, secure fax).</p>
<p><u>Section 4.0</u> – Bureau Follows Six Step Incident Handling Process</p>	<p>4.1.4 – The eradication process.</p>
<p><u>Section 4.2.4</u> – Reporting incidents As Closed When Resolved</p>	<p>“Bureau CSIRC reports incidents as closed when resolved.”</p>
<p><u>Section 4.2.4</u> –Reporting subsequent incident information to TCSIRC</p>	<p>“Bureau reports any subsequent incident information to TCSIRC.”</p>
<p><u>Section 5.1</u> – Bureau CSIRC distributes advisories and bulletins to appropriate bureau personnel</p>	<p>“Bureau CSIRC distributes TCSIRC advisories and bulletins to the appropriate bureau personnel, network operations center, systems administrators, and information system security officers.”</p>

Source: OIG Analysis of Treasury IT Security Program (TD P 85-01)



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

June 22, 2005

MEMORANDUM FOR LOUIS C. KING
DIRECTOR, INFORMATION TECHNOLOGY AUDITS
OFFICE OF INSPECTOR GENERAL

FROM: Gregory D. Carper
Associate Director
(Chief Financial Officer) *Gregory D. Carper*

SUBJECT: Draft Audit Report – BEP's Computer Security Incident
Response Capability Needs Improvement

Thank you for the opportunity to review the Office of Inspector General's (OIG) draft audit report "BEP's Computer Security Incident Response Capability Needs Improvement." Comments regarding the report recommendations follow.

Recommendation 1: The Chief Information Officer should ensure that current BEP CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01.

Comment: Requirements which were changed from Treasury Directive Publication (TDP) TD P 71-10 to TD P 85-01 have been updated in the revised Bureau of Engraving and Printing (BEP) Policy and the BEP Computer Security Incident Response Capability (CSIRC) Manual. Even though revisions to TD P 85-01 are still ongoing at the Treasury level, BEP continues to refine and update all policies and procedures on a regular basis in compliance with National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), Treasury guidance, and best practices.

The BEP procedures were consistent with Treasury policy, TD P 71-10, when written. Revised procedures are consistent with Treasury and NIST guidance, and best practices. All of the following sections have been modified to meet current guidance.

Section 2.6	CSIRC definitions and classifications.
Section 2.7.6	Bureau CSIRC responsibilities.
Section 3.2.1	Individual (significant) incident reporting.
Section 3.2.2	Monthly (minor) incident reporting.
Section 3.3.1	Significant incident reporting methods.
Section 4.1.4	Eradication process for incident handling.

Appendix 4 Management Comments

Section 4.2.4	Reporting incident as closed when resolved.
Section 4.2.4	Reporting subsequent incident information to Treasury's Computer Security Incident Response Center (TCSIRC).
Section 5.1	Bureau CSIRC distributes advisories and bulletins to appropriate Bureau personnel.

We consider this recommendation implemented.

Recommendation 2: The Chief Information Officer should ensure that BEP's "Security Awareness and Training Policy" is updated and incorporates the guidance established by TD P 85-01.

Comment: At the time of the OIG audit, the reference to TD P 71-10 may not have been changed to TD P 85-01. However, at that time and currently, BEP's Awareness and Training Policy, and the security awareness and training programs do reflect current NIST, Federal Information Security Management Act, and Treasury policy and content. The reference to TD P 85-01 has been incorporated into the Security Awareness and Training Policy. We consider this recommendation implemented.

Recommendation 3: The Chief Information Officer should ensure that an IDS is established for BEP's computer operations to ensure that computer security incidents are being accurately identified and reported.

Comment: BEP has relied on the Treasury Intrusion Detection System (IDS), establishing and implementing strong policy, and dual firewalls at the Treasury Communication System (TCS) and the BEP perimeter to protect the network. However, we are currently evaluating host-based IDS's and will be implementing a system following product comparison, evaluation, and testing. We expect the evaluation to be completed and the system installed by March 2006.

Recommendation 4: The Chief Information Officer should ensure that computer security incident information is consistently reported to TCSIRC by the fifth calendar day of each month.

Comment: Both cases of late reporting cited in the report were exceptions to BEP's normal on-time monthly reporting. In both cases, TCS was notified in advance and concurred with the day late reporting. From April 2004 through May 2005, BEP met all date reporting requirements except for one month, October 2004, in which the report was delayed due to illness of the BEP CSIRC reporter. We consider this recommendation implemented.

If you have any questions regarding our comments, please call me on (202) 874-2020.

Office of Inspector General

Louis C. King, Director
Joseph A. Maranto, III, IT Audit Manager
George Prytula, III, IT Audit Manager
Cedric E. Hammond, Sr., Program Analyst
Susan R. Sebert, Referencer

Department of the Treasury

Office of the Chief Information Officer
Office of Accounting and Internal Control

Bureau of Engraving and Printing

Chief Information Officer
Office of Critical Infrastructure and IT Security
Office of Management Control

Office of Management and Budget

Office of Inspector General Budget Examiner