



Audit Report



OIG-05-040

INFORMATION TECHNOLOGY: Mint's Computer Security Incident Response Capability Needs Improvement

July 13, 2005

Office of
Inspector General

Department of the Treasury

Contents

Audit Report	3
Results In Brief.....	4
Background	4
Findings and Recommendations	5
Mint’s CSIRC Policy And Procedures Need To Be Updated	6
Recommendations.....	8
Mint’s Computer Security Incident Reporting Was Not Complete	8
Recommendation	11
Mint’s Software Patch Management Process Needs Improvement.....	11
Recommendations.....	14

Appendices

Appendix 1: Objective, Scope, and Methodology	16
Appendix 2: Overview of Treasury’s CSIRC Structure	17
Appendix 3: Management Comments	19
Appendix 4: Major Contributors	23
Appendix 5: Report Distribution.....	24

Abbreviations

CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Capability
FISMA	Federal Information Security Management Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act
IDS	Intrusion Detection System
IT	Information Technology
Mint	United States Mint
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIS	Office of Information Security

Contents

OIT	Office of Information Technology
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*

July 13, 2005

Jerry Horton
Chief Information Officer
United States Mint

The Office of Inspector General's (OIG) Annual Audit 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 incidents 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 United States Mint (Mint) established an adequate CSIRC process. To accomplish this objective, we: (1) interviewed Mint 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 the Mint established a CSIRC and a software patch management function, its computer security incident reporting process needs improvement. For instance, we identified that: (1) CSIRC policy and procedures need to be updated; (2) security incidents were not being completely reported; and (3) necessary documentation for its patch management system was not being retained.

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

1. Current Mint CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01.
2. Help Desk procedures are created that clearly define requirements for communications with the Office of Information Security (OIS) when an incident is discovered.
3. Complete computer security incident data is collected from all existing internal and external sources and is consistently reported to the Treasury Computer Incident Response Center (TCSIRC) on a monthly basis.
4. Current software patch management policy and procedures are updated and incorporate penetration testing guidance established by TD P 85-01.
5. All security bulletin patches retain appropriate configuration change request and testing documentation.
6. All applicable security bulletin patches are applied, and written justification is retained for those that are not applied.
7. All configuration change requests are included in the patch tracking system.

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 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 intrusion detection system (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.

Prior to our audit, OIS did not have a full-time manager for the Mint's CSIRC function. However, during the audit, an Operations Division Chief was appointed and was assigned the responsibility to manage the Mint's CSIRC function.

Findings and Recommendations

Although deficiencies existed in its current CSIRC process, we identified areas where the Mint was taking appropriate steps in

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

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

establishing an adequate CSIRC and software patch management function. For example:

- Mint established a full-time CSIRC function operated by the OIS.
- Mint's CSIRC function distinguishes between computer security "events"⁴ and computer security "incidents."⁵ Further, computer security incidents are reported on a monthly basis.
- Mint established a full-time software patch management function to address computer security vulnerabilities. The software patch management function is operated by the Office of Information Technology (OIT).
- The software patch management function subscribes to relevant hardware and software vulnerability alert services.
- The OIT maintains a dedicated lab used for testing patches prior to implementation.
- Mint's software patch management function is integrated with the configuration management process, which includes a change control board that reviews and approves software patches.
- The OIS developed an end user IT security awareness training program in which aspects of the CSIRC function are incorporated.

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

Mint's policy and procedures relating to CSIRC were not current with Treasury guidance. More specifically, (1) current CSIRC policy was based on outdated Treasury policy; (2) current CSIRC procedures did not incorporate all required aspects of Treasury's current IT security policy; and (3) Mint's Help Desk policy does not address handling computer security incidents. By not updating current policy and procedures, the Mint cannot ensure that IT security personnel will address computer security incidents appropriately.

⁴ Per TD P 85-01, an "event" is a notable occurrence, not yet assessed, in a computing or telecommunications system or network that may affect that system or network.

⁵ Per TD P 85-01, an "incident" is the violation of an explicit or implied security policy in a computing or telecommunications system or network.

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

We found that although the Mint established a policy regarding its CSIRC process, this policy was not based on current Treasury policy. The Mint's current policy⁶ establishes guidelines for responding to and reporting information technology incidents, however, the policy is based on Treasury's 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. By not incorporating the policy guidance mandated by TD P 85-01, Mint CSIRC policy is not current with Treasury's IT security policy.

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

We also found that Mint established procedures regarding its CSIRC process. Mint's current procedures⁷ provide guidance for recognizing and identifying IT security incidents. Further, the procedures assist in defining security incidents, as well as how to respond to IT events that become security incidents. After comparing Mint's CSIRC procedures with TD P 85-01, we found that the procedures did not require Mint to:

- Update TCSIRC every four hours after an initial incident report is filed, until the incident is resolved; and as new information about the incident is discovered.⁸
- Specify approved methods for Mint's CSIRC to deliver unclassified system incident data to TCSIRC.⁹
- Specify approved methods for Mint's CSIRC to deliver critical infrastructure protection asset incident data to TCSIRC.¹⁰
- Forward to TCSIRC, any relevant information that becomes available after an incident is closed.¹¹

⁶ Mint Directive 9C-5, *IT Security Incident Response and Reporting Policy*, dated May 2002.

⁷ *U.S. Mint IT Security Incident Prevention and Response Procedures*, dated May 28, 2004.

⁸ Part 1—Sensitive Systems, Section 6.2.2.1 of TD P 85-01.

⁹ Part 1—Sensitive Systems, Section 6.2.2.6 of TD P 85-01.

¹⁰ Part 1—Sensitive Systems, Section 6.2.2.7 of TD P 85-01.

By not incorporating the policy guidance mandated by TD P 85-01, the Mint's CSIRC procedures are not current with Treasury's IT security policy.

Mint's CSIRC Procedures Do Not Address Handling Computer Security Incidents For Its Help Desk

The Mint did not establish procedures requiring Help Desk personnel to notify OIS when a suspected incident is discovered. However, during the audit, OIS acknowledged that procedures would be created to address this deficiency. By not establishing procedures requiring Help Desk personnel to notify OIS when an incident is discovered, Mint increases the risk that detected incidents will go unreported.

Recommendations

The CIO should ensure that:

1. Current Mint CSIRC policy and procedures are updated and incorporate the guidance established by TD P 85-01.
2. Help Desk procedures are created that clearly define requirements for communications with the OIS when an incident is discovered.

Management Response Management agreed with the recommendations and has implemented or is in the process of instituting corrective measures.

OIG Comment The actions taken and/or planned by the Mint's Office of Information Security are responsive to the intent of our recommendations.

Finding 2

Mint Computer Security Incident Reporting Was Not Complete

The Mint security incidents were not being completely reported. Specifically, we found that incidents involving the Mint's firewall,

¹¹ Section 6.3.2.4 of TD P 85-01.

IDS, e-mail server virus detection software, Help Desk, and IT equipment thefts were not being accurately and completely reported. By not completely identifying all computer security incidents, the Mint is underreporting its actual security incidents.

Firewall Log Incidents Were Not Accurately Reported

The Mint was not reporting all firewall¹² log incidents to TCSIRC. For the month of August 2004, the Mint reported zero “unsuccessful access or penetration attempt” incidents to TCSIRC. Mint currently has 15 firewalls deployed for its various network systems. Each firewall produces a continuous log file of relevant network events that the firewall has evaluated and processed. The amount of data collected in these firewall event logs is substantial.

We received the data for one of the firewalls event log files for the month of August 2004. Because of the large volume of event log data, only the first and last days of August 2004 were examined. The firewall event log files identified 21,110 and 65,940 events for both of these days, respectively. From these events, we identified that 1,567 and 7,315 were categorized as actual computer security incidents. These numbers represent unsuccessful access or penetration attempts and are reportable per TD P 85-01.

IDS Log Incidents Were Not Completely Reported

Because OIS does not research medium and low severity IDS events¹³, they were unable to completely determine how many actual computer security incidents occurred at the time of our audit. 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.

The commercial provider for the Mint’s CSIRC function classifies all IDS events as high, medium, or low severity according to its own internally developed criteria. When an IDS event is classified in the

¹² A firewall allows authorized network traffic to pass through the device and onto its specified destination and is used to block unauthorized attempts to access IT resources.

¹³ For the two days that we reviewed, most of Mint’s IDS event log data falls in these two categories.

high severity category, the commercial provider verbally alerts OIS personnel, who research the event and verifies all relevant information. If OIS determines that a high priority IDS event is an actual computer security incident, then it is reported to TCSIRC as such.

We selected our sample of IDS event log data that corresponded to the firewall that was discussed in the previous section. We selected the month of August 2004 for our review. Because of the large volume of event log data, only the first and last days of August 2004 were examined. We found that 15,764 and 15,270 total events were recorded for these days, respectively. However, since OIS does not research medium and low severity IDS events, the total number of incidents could not be determined.

E-mail Server Anti-Virus Incidents Were Not Reported

The Mint was not reporting virus detection (and removal) incidents to TCSIRC. For the month of June 2004, Mint reported zero virus detection (and removal) incidents to TCSIRC. Mint's e-mail system is administered by five Microsoft Exchange servers. All five servers process an anti-virus program capable of removing e-mail viruses and unwanted e-mail (i.e., Spam). These servers also produce a continuous log file showing e-mail virus removal activity. We utilized the results of these logs for all five servers and found that 54 virus removal incidents were identified.

Mint's Help Desk Security Incidents Were Not Reported

The Mint was not reporting Help Desk security incidents to TCSIRC. For the month of March 2004, the Mint reported zero computer security incidents to TCSIRC. Our review of the Help Desk tracking system showed that of the 3,120 tickets generated for March 2004, 50 tickets identified potential IT security issues. Some of these issues included actual viruses detected and removed by the Microsoft Exchange E-mail server's anti-virus program; and a suspected virus was identified after a virus scan was performed. In addition, we identified tickets listing potential IT security problems. However, these tickets contained incomplete or inconclusive information regarding the follow-up and resolution of the issue.

Mint IT Equipment Theft Incidents Were Not Reported

The Mint reported zero IT equipment thefts to TCSIRC for the month of March 2004. However, Mint Police case files identified that one case of IT equipment theft was reported for March 2004. This case involved the theft of six personal computers from a Mint site in the Washington, DC area.

Recommendation

The CIO should ensure that:

3. Complete computer security incident data is collected from all existing internal and external sources ensuring that data is consistently reported to TCSIRC on a monthly basis.

Management Response Management substantially agreed with the recommendation and is in the process of instituting corrective measures to address several of the issues detailed in our report. However, the Mint stated that they believe that the reporting requirement in TD P 85-01 to report all quarantined files would have a significant impact on their resource utilization. The Mint has requested an Exception to Policy for reporting e-mail server anti-virus incidents, and they have recommended that the reporting requirement be deleted from TD P 85-01. They are currently waiting for a response to this request for an exemption. If the exemption is granted, the Mint will report only significant malicious application incidents. If the exemption is denied, the Mint will report all incidents as required by TD P 85-01.

OIG Comment We believe management should implement our recommendation as stated.

Finding 3

Mint's Software Patch Management Process Needs Improvement

Although the Mint has established a process for managing its software patch management function, improvement is still needed. For example, the Mint's current software patch management policy

was not complete. Also, Mint was not retaining the necessary information for its patch management tracking system.

Software Patch Management Policy Was Not Complete

The Mint established policy and procedures for its software patch management process. The policy and procedures were in compliance with TD P 85-01, with the exception of penetration testing follow-up. TD P 85-01 requires that bureaus ensure that vulnerabilities discovered during penetration testing are repaired and that any damages incurred during the interim are mitigated. The Mint's current policy and procedures do not address this issue. Without establishing guidance requiring adequate follow-up on vulnerabilities identified during penetration testing, Mint systems could remain vulnerable to security attacks.

Supporting Documentation For Mint's Patch Tracking System Is Incomplete

As part of its CSIRC process, the Mint established a software patch management function. This process is performed by the OIT in conjunction with the Mint's change control board. The software patch management cycle consists of: (1) receiving alerts of possible IT security vulnerabilities; (2) logging the alerts into a tracking system; (3) assessing the relevance of alerts to current IT infrastructure; (4) forwarding relevant alerts and patches to the internal configuration management process; (5) testing proposed software patches; (6) receiving final configuration management approval for installation; and (7) installing software patches and tracking results.

We reviewed the OIT's patch tracking system and patch processing cycle and found that documentation did not exist for some of the security bulletin patches we reviewed. For example, we found that some of the Microsoft Security Bulletin Patches were installed but lacked appropriate configuration change request documentation, as well as testing documentation. We also found examples where Microsoft Security Bulletin Patches that should have been installed, were not. Further, no explanation was documented on why the decision was made not to install these patches. Finally, we found

that some Mint configuration change requests were not entered in the patch tracking system.

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:

- 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 a complete CSIRC and software patch management process, the Mint runs the risk of not accurately identifying and accounting for all its computer security incidents. As a result, the Mint may understate mandated CSIRC reporting requirements such as those identified as part of FISMA. For the Government Information Security Reform Act (GISRA) FY 2002 reporting (the precursor to FISMA), the Mint reported zero computer security incidents. For FISMA FY 2003 reporting, the Mint only reported one incident. This discrepancy occurred because the Mint was only reporting significant (excluding minor) incidents for their GISRA and FISMA reports. By continuing to report incomplete and inconsistent information, the Mint cannot ensure that computer security incidents are being reported correctly.

Recommendations

The CIO should ensure that:

4. Current software patch management policy and procedures are updated and incorporate penetration testing guidance established by TD P 85-01.
5. All security bulletin patches retain appropriate configuration change request and testing documentation.
6. All applicable security bulletin patches are applied, and written justification is retained for those that are not applied.
7. All configuration change requests are included in the patch tracking system.

Management Response Management agreed with the recommendations and has implemented or is in the process of instituting corrective measures.

OIG Comment The actions taken and/or planned by the Mint's Office of Information Security are responsive to the intent of our recommendations.

* * * * *

I would like to extend my appreciation to the Mint 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 4.

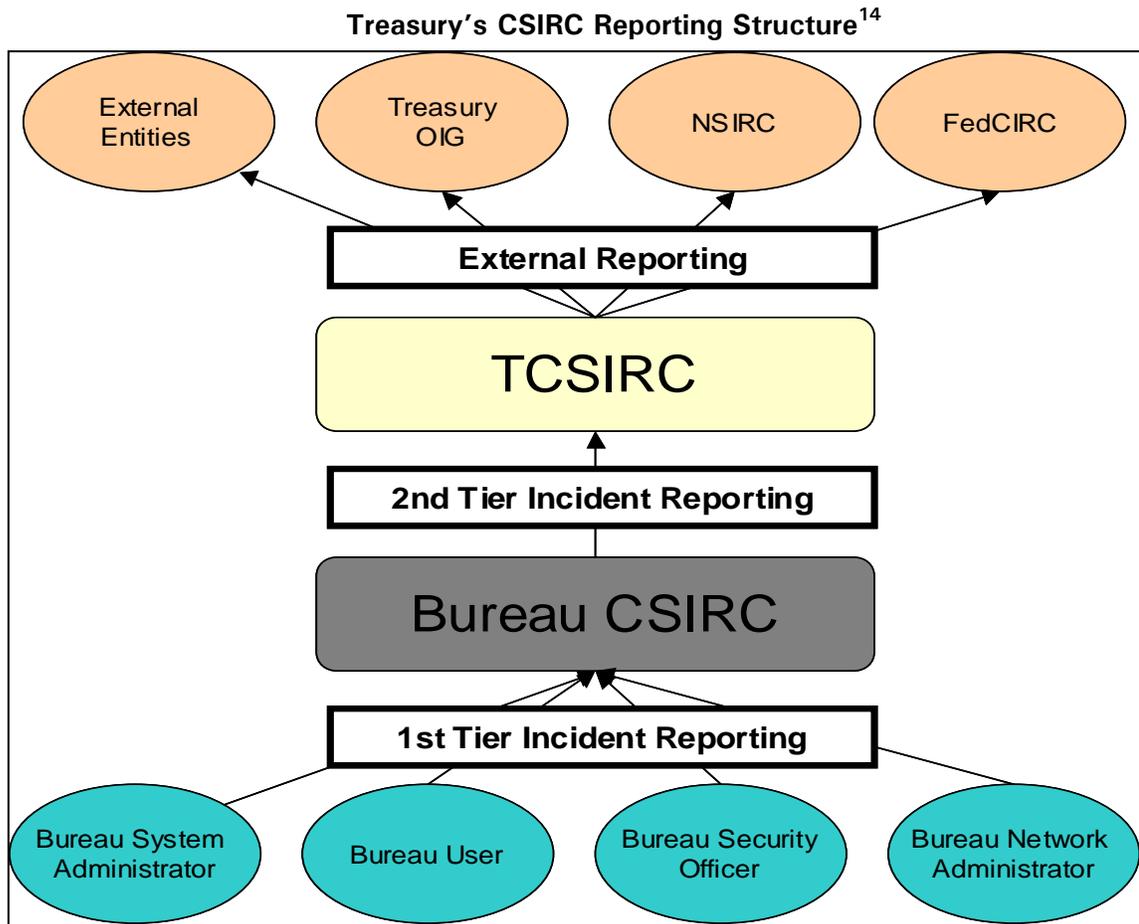
/s/

Louis C. King
Director, Information Technology Audits

The objective of this audit was to determine if the Mint established an adequate CSIRC process. This objective was accomplished by determining if the Mint established and implemented CSIRC policy and procedures compliant with Treasury and OMB criteria, as well as ensuring an adequate CSIRC process. We performed this audit by: (1) interviewing appropriate OIS and OIT 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 the Mint'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.
- Government-wide information sharing of threats, incidents, and trends to support computer security planning and operations.

¹⁴ As of September 2003, the United States Computer Security Readiness Team (i.e., US-CERT) replaced FedCIRC in protecting the nation's Internet infrastructure against cyber attacks.

The following events are defined as computer security incidents and should be reported to TCSIRC:

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 Impact	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)

Appendix 3
Management Comments



DEPARTMENT OF THE TREASURY
UNITED STATES MINT
WASHINGTON, D.C. 20220

MEMORANDUM FOR LOUIS C. KING
DIRECTOR, INFORMATION TECHNOLOGY AUDITS

FROM: Jerry Horton 
Chief Information Officer

DATE: June 30, 2005

SUBJECT: Treasury Office of Inspector General Discussion Draft Audit
Report "The Mint's Computer Security Incident Response
Capability Needs Improvement"

The United States Mint has reviewed the Treasury Office of Inspector General's (OIG) Discussion Draft Audit Report "The Mint's Computer Security Incident Response Capability Needs Improvement." We appreciate the OIG's observations and recommendations intended to improve the quality and efficiency of the Mint's Computer Security Incident Response Capability (CSIRC).

The attached comments are forwarded for your consideration. We appreciate the opportunity to comment on this Discussion Draft Report. I am requesting that you include our complete responses in your final report. If you have any questions, please do not hesitate to call me.

Attachment

1

Appendix 3
Management Comments

Management Response to Office of Inspector General Discussion Draft Report "The Mint's Computer Security Incident Response Capability Needs Improvement"

FINDING 1: MINT'S CSIRC POLICY AND PROCEDURES NEED TO BE UPDATED

1. Mint's CSIRC Policy Is Not Based On Current Treasury Policy
2. Current CSIRC Procedures did not incorporate all of the required aspects of Treasury's current IT security Policy
3. Mint's CSIRC Procedures Do Not Address Handling Computer Security Incidents For Its Help Desk

United States Mint OCIO/OIS Response to Item 1: The United States Mint acknowledges the observation that portions of the CSIRC do not directly correspond to CSIRC policies identified in TDP 85-01. OIS is conducting a policy review. The review is scheduled to be completed by December 2005.

United States Mint OCIO/OIS Response to Item 2: The United States Mint acknowledges the observation that portions of the Mint's CSIRC procedures do not directly incorporate aspects of Treasury's IT security Policy identified in TDP 85-01. To address this observation, OIS has reviewed and published revised procedures, dated April 2005, which accurately reflect current TDP 85-01 guidance for security incident response.

United States Mint OCIO/OIS Response to Item 3: The United States Mint acknowledges the observation that the Help Desk procedures do not address the coordination of computer security incident handling with OIS. The Office of Information Technology (OIT), in coordination with OIS, has developed and will publish Standard Operating Procedures (SOP) for security incident handling. We expect complete implementation of these procedures by December 2005. In addition, the INFOSEC Awareness Training Program has been updated to address security incident response. OIT and OIS will implement training sessions to reinforce security incident protocols on a recurrent basis.

FINDING 2: MINT SECURITY INCIDENT REPORTING WAS NOT COMPLETE

1. Firewall Log Incidents Were Not Accurately Reported
2. IDS Log Incidents Were Not Completely Reported
3. E-mail Server Anti-Virus Incidents Were Not Reported
4. Mint's Help Desk Security Incidents Were Not Reported
5. Mint IT Equipment Theft Incidents Were Not Reported

United States Mint OCIO/OIS Response to Item 1: The United States Mint acknowledges the observation that the Firewall Log events were not completely reported. OIS has coordinated with the managed service security provider (MSSP) for the United States Mint intrusion detection system (IDS) program to

Appendix 3 Management Comments

modify the contract with the MSSP to support firewall log data processing for the internal firewalls. Once approved and implemented, this will allow firewall log data from a "syslog" server to be sent in near-real time to the MSSP for correlation with United States Mint's IDS sensor data. This near-real time correlation will provide additional insight into the security posture of those unique interfaces being addressed by these internal firewalls. Estimated completion time is September 2005.

United States Mint OCIO/OIS Response to Item 2: The United States Mint acknowledges the observation that the IDS Log Incidents were not completely reported. OIS will conduct an in-depth analysis of functional capabilities of the systems and networks currently under IDS protection to create a baseline, and fine-tune the IDS to minimize the large set of alerts. The correlation of firewall log data at Headquarters will assist in the fine-tuning of Headquarters IDS data. Estimated completion time is September 2005.

United States Mint OCIO/OIS Response to Item 3: The United States Mint acknowledges the observation that E-Mail Server Anti-Virus incidents were not reported. The observation refers to anti-virus "malware" captured via Exchange attachment checking. In addition to server based antivirus software, United States Mint relies on Symantec Anti-Virus Corporate Edition (SAVCE) software to protect servers and clients. United States Mint also has implemented an anti-spam solution, which "quarantines" email that may have malicious links or script code embedded into them. Once United States Mint implements the planned anti-spyware technical solution, it is anticipated that the software will also quarantine malware. In light of all these technologies capturing malware, it is anticipated that complying with the TDP 85-01 requirement to report all quarantined files would significantly impact resource utilization. Additionally, the US-CERT Concept of Operations for Cyber Security Incident Handling, version 3.2, dated April 2005, defines the category Malicious code in table 3-3 (titled Federal Agency Incident Categories) as follows: "Successful installation of malicious software (i.e. virus, worm, Trojan horse, or other code-based malicious entity that infects an operating system or application. Agencies are NOT required to report malicious logic that has been successfully quarantined by antivirus (AV) software." Based upon the resources required to track and report quarantined malware, and the US-CERT definition referenced above, the United States Mint has (1) requested an Exception to Policy for reporting E-Mail Server Anti-Virus incidents (Virus quarantines and other types of malware quarantined by Mint software), and (2) recommended the reporting requirement be deleted from TDP 85-01. The Mint is currently awaiting a response to our request for an exception to policy from Treasury DO. If Treasury DO concurs with the Mint's request, we will report only significant malicious application (Virus, Worms, etc) incidents. If Treasury DO non-concurs with the Mint's request we will report all incidents as required by TDP 85-01.

Appendix 3 Management Comments

United States Mint OCIO/OIS Response to Item 4: This observation is being addressed as identified in Finding 1, item 3.

United States Mint OCIO/OIS Response to Item 5: The United States Mint acknowledges the observation that IT equipment theft incidents were not reported to TCSIRC. Operationally, all physical related security events are managed by the Office of Protection. Their protocol does not contain a reporting requirement to notify OIS on physical IT related security events. To address this observation, the Mint will coordinate with Office of Protection and reinforce the need to address the data sensitivity aspect of IT related thefts. In addition, Help Desk standard operating procedures were updated so that when a user reports missing equipment, a security incident report is created. To supplement the Help Desk's standard operating procedures, the United States Mint's and using INFOSEC awareness training, users are reminded to contact both Help Desk and the Office of Protection when reporting computer equipment theft.

FINDING 3: MINT'S SOFTWARE PATCH MANAGEMENT PROCESS NEEDS IMPROVEMENT

1. Software Patch Management Policy Was Not Complete
2. Supporting Documentation For Mint's Patch Tracking System Is Incomplete

United States Mint OCIO/OIS Response to Item 1: The United States Mint acknowledges the observation that the United States Mint's patch management procedures do not adequately address the requirement to mitigate deficiencies discovered during penetration testing, or repair any damages incurred as a result of the vulnerability. All Mint penetration/vulnerability testing is conducted with an emphasis on non-invasive techniques focused on identifying, classifying and reporting discoveries to system owners. To address this observation, the Mint will review its patch management procedures and will enhance existing penetration testing follow-up procedures to ensure complete reporting. We anticipate implementation of the procedural enhancements by December 2005.

United States Mint OCIO/OIS Response to Item 2: The United States Mint acknowledges the observation that supporting documentation for Mint's patch tracking system is incomplete. While the Mint adequately performs the auditing function, the OIG observation identified that the documentation for patches purposefully not applied to systems were incomplete. To address this observation, the Mint will review and modify its current procedures for the Patch Tracking System to include a documentation methodology for patches purposefully excluded from implementation into production. Formal implementation of these procedures will occur prior to December 2005. Additionally, OIS has implemented an enterprise vulnerability assessment tool to conduct recurring network scans of all Mint networks to discover unpatched systems. OIS then identifies and reports improperly patched systems to OIT staff so they can manually check and patch affected systems, as appropriate.

Office of Inspector General

Louis C. King, Director
Joseph A. Maranto, III, IT Audit Manager
George Prytula, III, IT Audit Manager
Susan R. Sebert, Referencer

Department of the Treasury

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

United States Mint

Office of Information Security
Office of Information Technology

Office of Management and Budget

Office of Inspector General Budget Examiner