BUREAU OF ENGRAVING AND PRINTING

CIRCULAR

No. 10-08.22

DATE May 21, 2001

COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)

1. PURPOSE AND SCOPE. This policy ensures that the Bureau of Engraving and Printing (BEP/Bureau) complies with all laws and regulations relating to the identification, reporting, and response to computer and network security breaches, viruses, and web attacks. It applies to all personnel (Bureau employees, contractors, students), Bureau networks, networked computers, and computer terminals, laptops, or other data processing or communication devices owned, issued, or controlled by the Bureau.

2. POLICY. The Bureau will provide a coordinated response to threats to its information technology assets and information systems. The Bureau will provide 24 hours a day, seven days a week incident identification and reporting capability which will maintain an ongoing program to identify potential threats, respond to attacks on its communication networks or individual computers and computer facilities, and report incidents to the Department of the Treasury and other agencies or appropriate organizations.

3. BACKGROUND. Computer and network security has increasingly received high profile attention as computer and network security breaches in the private sector and in the Government have continued to make national and international headlines. Federal Government regulations and the implementation of these regulations in Federal organizations have been receiving a great deal of Congressional and public scrutiny. As the Government comes to rely more and more on networks and computerized information as a result of the provisions of the Government Paperwork Reduction Act and other legislation, this scrutiny will continue.

There is now a concerted effort within the Government to bring all systems and policies in compliance with national policies. The Department of the Treasury has established a Computer Security Incident Response Capability (CSIRC) for identifying threats, providing advice to Bureaus on responding and investigating, and for disseminating information of security breaches to national organizations such as the Federal Computer Incident Response Capability (FedCIRC) and the National Security Incident Response Center (NSIRC).

4. REFERENCES.

Critical Infrastructure Protection, Presidential Decision Directive 63, May 1998.

Computer Security Incident Response and Reporting, Department of the Treasury Security Manual TD P 71-10, Section 5B (in draft).

"Security of Federal Automated Information Systems," OMB Circular A-130, Appendix III (revised October 2000).

National Plan for Information Systems Protection, January 7, 2000.

5. DEFINITIONS. Attachment 1 provides a list of the definitions of computer security incidents. These incidents may be either "significant" or "minor."

a. Significant incident – any IT security related incident that slows or prevents the use of a computer, a network, or a system for longer than 30 minutes, or which impacts another bureau, agency or organization.

b. Minor incident – any IT security related incident that slows or inconveniences users in the use of a computer, a network or a system, but does not prevent them from using information system resources.

6. RESPONSIBILITIES.

a. The Associate Director (Chief Information Officer) of the Bureau provides oversight of the BEP incident response program. These responsibilities include assuring that the Bureau complies with Treasury policy and advocating a strong CSIRC program at the Bureau executive management level.

b. The Manager, Information Technology Security Division, is the primary BEP point of contact (POC) for reporting computer security incidents (the Manager, ITSD, will also designate at least one secondary POC who can be reached after normal work hours if necessary). This individual has the responsibility for:

(1) performing an initial investigation to verify the occurrence of a security compromise;

(2) notifying Treasury CSIRC of significant incidents:

(a) alerting Treasury CSIRC of the sensitivity of the compromised information and the nature of the incident as soon as possible, but no later than four hours after the event (BEP information will be considered either nonsensitive or sensitive but unclassified. Any information which is under a National Security Classification will be handled separately).

(b) incident reporting will primarily be through the Department of the Treasury Incident Reporting System (INREPSYS), although e-mail, telephone, fax, or written memorandum may be used if necessary. The security of the method of transmission must be appropriate to the sensitivity of the information reported.

(3) initiating incident evaluation, and assisting and advising system owners, administrators and points of contact (POCs) in response and recovery operations to Bureau systems and computers. Advising and assisting system owners and administrators in implementing appropriate countermeasures;

(4) performing internal investigations or, upon request, assisting other Bureaus or the Department of the Treasury in incident investigations or with technical assistance;

(5) briefing Bureau executives and managers on incidents; and

(6) tracking and reporting on incidents and the outcome of completed investigations, in support of BEP or the Department of the Treasury CSIRC investigations. Providing a monthly report of all incidents, including minor incidents, to the Department of the Treasury.

c. Improvements in preventing significant damage from information security incidents and ensuring more effective and faster responses will be directly affected by increased training of security and IT professionals and the Bureau employee population. The Manager, ITSD, shall:

(1) Identify points of contact within each Office or major program area with the responsibility for reporting incidents and distributing information within that functional area;

(2) identify training topics and subjects which are needed to improve technical and administrative response capability; and

(3) coordinate with system owners and administrators to develop a comprehensive incident response training program which will include exercises as an outcome of training. Ensure that this training is provided to IT security staff, system administrators, managers, and system users. Appropriate identification of incidents and adequate reporting are responsibilities of all IT professionals and those in the user community.

d. System owners or system administrators for systems, equipment or applications, shall:

(1) designate a point of contact (POC) for each Office or major function with the responsibility for reporting incidents and distributing information relating to computer security and incident reporting within their functional area;

(2) immediately notify the Manager, ITSD, of any security incident or compromise of information; and

(3) coordinate with the Manager, ITSD, in responding to security incidents and in initiating recovery efforts. This also includes developing, testing and implementing appropriate countermeasures.

e. All Treasury and Bureau employees, other Government employees or contractors who are users of Department or Bureau information systems or computers shall notify the Help Desk immediately upon suspecting that a computer system, network, stand-alone or laptop computer has been compromised. This compromise could be any of the incidents defined in Attachment 1 or a related incident. Any individual who has been authorized access to any Bureau networks, e-mail, or other computer access has the obligation to immediately cease using the computer and report the incident.

7. OFFICE OF PRIMARY RESPONSIBILITY. Associate Director (Chief Information Officer).

Ronald W. Falter
Associate Director (Chief Information Officer)

DISTRIBUTION: E

Computer Security Incident Response Capability
Attachment 1
Definitions of Treasury Computer Security Incidents

1. Malicious Code/Malicious Logic – These events are performed by crackers/hackers in an attempt to gain privileges and/or information, to capture passwords, and to modify audit logs to hide unauthorized activity. The attempts include the use of active code such as viruses, Trojan horses, worms, and scripts. This category includes any virus or code that is intended to disrupt or annoy users.

2. Probes and Reconnaissance Scans – These events include probing or scanning networks for critical services or security weaknesses. They also include nuisance scans.

3. Unauthorized Access and Unsuccessful Attempts – These events include all successful unauthorized accesses and suspicious unsuccessful attempts.

4. Denial of Service Attacks – These events are attacks that affect the availability of critical resources such as e-mail servers, web servers, routers, gateways, or communication infrastructure.

5. Alteration/Compromise of Information – These events involve the unauthorized altering of information or incidents that involve the compromise of information.

6. Adverse Site Mission Impact – These events have significant impact on the mission of the site or operations but do not fall into any of the aforementioned categories.

7. Classified System Incident – These events involve a system used to process national security information or involve classified information on any system not certified for that level of classified information.

8. Loss or Theft of Equipment – These events must be reported to the CSIRC to determine the potential compromise of sensitive material. This includes the compromise of user accounts and passwords that could allow unauthorized persons to access Treasury computing resources, or names or case information that could compromise an investigation. The CSIRC priority is the data that may have been lost or stolen, rather than on the hardware itself.