

***Computer Security Incident Response Capability (CSIRC)
Procedures***



**ASSOCIATE DIRECTOR
(CHIEF INFORMATION OFFICER)**

DATE July 31, 2002

**COMPUTER SECURITY INCIDENT RESPONSE CAPABILITY (CSIRC)
MANUAL**

1. The BEP Computer Security Incident Response Capability Manual identifies resources necessary to prevent, identify, respond to, resolve, and report computer security incidents that may adversely affect the Bureau's information technology resources and therefore the Bureau's ability to accomplish its mission.

2. The BEP CSIRC Manual covers incident response activities for all BEP information systems, including those administered by the Chief Information Officer (CIO), other directorates, or contractors. BEP CSIRC policy and procedures apply to all persons who use or administer BEP information technology resources.

3. The Office of Primary Responsibility for the BEP CSIRC is the Associate Director (CIO).

<SIGNED>

Thomas A. Ferguson
Director

DISTRIBUTION - C

DATE July 31, 2002

BEP CSIRC PROCEDURES – TABLE OF CONTENTS

1.0 Introduction.....	1
1.1 Background.....	1
1.2 References.....	1
1.3 BEP CSIRC Mission Statement.....	2
1.4 Purpose and Scope.....	2
1.5 Objectives of the BEP CSIRC.....	2
2.0 CSIRC Organization.....	3
2.1 BEP CSIRC Management.....	3
2.2 BEP CSIRC Extended Team.....	5
2.3 Incident Response Support Team.....	6
2.4 CSIRC Relationships with Internal & External Organizations.....	6
3.0 CSIRC Services.....	7
3.1 Incident Prevention.....	7
3.2 Incident Detection.....	8
3.3 Incident Response.....	9
3.4 Incident Tracking and Reporting.....	9
4.0 Incident Response Guidelines.....	10
4.1 Incident Priority Levels.....	10
4.2 The Five Phases of the Incident Response Process.....	11
4.3 Generic Response Guidelines.....	13
5.0 Incident Response Process.....	14
5.1 Initiating the Incident Response Process.....	14
5.2 Escalation Levels.....	15
6.0 Follow Up Assessment.....	18
7.0 Treasury CSIRC Reporting.....	19
8.0 Updating BEP CSIRC Procedures.....	20

EXHIBITS

Exhibit 1 – Incident Priority Levels.....	10
Exhibit 2 – Generic Response Guidelines.....	13

APPENDICES

Appendix A – Points of Contact.....	21
Appendix B - Sources of Incident Response & Advisory Information.....	22

DATE July 31, 2002

1.0 Introduction

1.1 Background

The Bureau of Engraving and Printing (Bureau/BEP) relies heavily on the availability, integrity, and confidentiality of information technology resources. Trends toward increasing system interconnections raise both productivity and risk of threats such as computer viruses, and intrusions.

Computer and network security has taken a much higher profile as computer and network security breaches, viruses, and web hacks have made international headlines. These situations can be costly in terms of the productivity lost when information is compromised, or unavailable to conduct business as usual; and resources are diverted from other projects to contain and recover damage to information systems. Additionally, they could have significant negative impact on the BEP's reputation.

Federal government regulations are now receiving Congressional and other high-level attention, as computer security becomes an important priority. Office of Management and Budget (OMB) Circular A-130 specifies Federal agencies will "Ensure there is a capability to provide help to users when a security incident occurs in the system and to share information concerning common vulnerabilities and threats." Presidential Decision Directive 63 (PDD-63) directs that each Department and agency will develop plans for protecting its own critical infrastructure.

The BEP Computer Security Incident Response Capability (BEP CSIRC) was established by BEP Circular 10-08.22, Computer Security Incident Response Capability policy, dated May 21, 2001 to address these issues in compliance with Treasury Security Manual, TD P 71-10.

1.2 References

- a. OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996.
- b. Presidential Decision Directive 63, "Protecting America's Critical Infrastructures," May 22, 1998.
- c. BEP Circular 10-08.22, "Computer Security Incident Response Capability," May 21, 2001
- d. Department of the Treasury Security Manual, TD P 71-10.
- e. Public Law 100-235, "Computer Security Act of 1987," January 8, 1988.
- f. Government Information Security Act of 2001, March 2001.

DATE July 31, 2002

1.3 BEP CSIRC Mission Statement

The BEP CSIRC mission is to protect, defend and when necessary, restore the availability, integrity, and confidentiality of the mission essential IT infrastructure, applications, and data of the Bureau of Engraving and Printing.

1.4 Purpose and Scope

The BEP Computer Security Incident Response Capability brings the necessary resources together in an organized manner to prevent, identify, respond to, resolve, and report computer security incidents that may adversely affect the BEP's information technology resources and BEP's ability to accomplish its mission.

The BEP CSIRC has primary jurisdiction over incident response activities for all BEP information systems, including those administered by the Chief Information Officer (CIO) or other directorates, or their contractors. BEP CSIRC policy and procedures apply to all persons who use or administer BEP information technology resources.

1.5 Objectives of the BEP CSIRC

The objectives of CSIRC Team are to:

- Provide a central organization to coordinate computer security incident response 24 hours a day, 7 days a week;
- Establish and maintain a structured incident reporting and response process;
- Serve as the central point for identifying and correcting computer system vulnerabilities;
- Keep current with the latest threats and vulnerabilities;
- Limit incident impact to customers and business partners;
- Prevent the use of BEP's systems in attacks against other systems (which could cause the Bureau to incur legal liability);
- Recover from computer security incidents;
- Facilitate communications with the Treasury CSIRC;
- Determine who initiated the incident;
- Determine how the incident occurred;
- Determine how to avoid future exploitation of the same vulnerability;
- Provide computer security guidance, assistance, and feedback in the form of "lessons learned" reports, trend analyses, alerts and advisories, and technical recommendations;
- Evaluate and strengthen in-place security measures;
- Evaluate security tools and products for their ability to maintain security standards;
- Update policies and procedures, as needed; and
- Comply with Federal, Treasury, and BEP policy.

DATE July 31, 2002

2.0 CSIRC Organization

The Associate Director (Chief Information Officer) 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.

The BEP CSIRC organization consists of the BEP CSIRC Management Team, supplemented by members of an Extended Team, and an Incident Response Support Team, as needed.

2.1 BEP CSIRC Management

CSIRC Management Team shall consist of the following officials or their designated representative(s):

Chair: Deputy CIO
Members: Manager, IT Security
Chief, Systems Development
Chief, IT Operations
Chief Technical Officer
Assistant CIO (Western Currency Facility (WCF))

BEP CSIRC Chair. The Deputy CIO, as BEP CSIRC chair, manages the BEP CSIRC organization, allocates resources, and is liaison to the Associate Director, CIO.

BEP CSIRC Management Team. The BEP CSIRC Management Team directs and activates resources for on-going and emergency CSIRC services. The team evaluates, implements and manages incident prevention, detection, and incident tools and methods. When vulnerabilities, threats, and incidents are identified they determine the course of action; and identify, mobilize and direct the necessary resources.

The Manager, Information Technology Security Division (ITSD), is the BEP Incident Coordinator and liaison to the Treasury CSIRC. The BEP Incident Coordinator is the primary point of contact for the Treasury CSIRC and is responsible for designating at least one alternate point of contact (POC) who, in addition to the BEP Help Desk, can be reached after hours in the event of an emergency.

The Manager, ITSD, is responsible for maintaining an acceptable level of risk with regard to the security of BEP IT resources. Primary CSIRC responsibilities include:

DATE July 31, 2002

- Monitoring for and alerting the BEP CSIRC to potential threats and vulnerabilities;
- Providing advice on technical and management measures to mitigate risk and/or recover from adverse incidents;
- Vulnerability tracking and reporting;
- Incident tracking and reporting;
- Coordinating all requests for outside assistance;
- Post-incident assessment and security enhancement; and
- Maintaining the CSIRC procedures.

The Chief, IT Operations, and Chief Technical Officer are responsible for the operation and implementation of the BEP IT infrastructure, respectively.

Their primary BEP CSIRC responsibilities include:

- Assessing impact of incidents and security measures on IT operations;
- Providing technical advice regarding the implementation of measures to contain damage and mitigate risk; and
- Providing technical specifications and status on the state of the current IT infrastructure. This includes implementing, documenting, and monitoring patches, workarounds and updates.

The Chief, Office of Systems Development (OSD), is responsible for maintenance of the Bureau's intranet, as well as development, programming support, and maintenance of many of the critical applications, systems, and databases, such as public sales and BEPMIS. The primary CSIRC responsibilities include:

- Assessing impact of incidents and security measures on web operations;
- Providing technical advice regarding the implementation of measures to contain damage and mitigate risk; and
- Providing technical specifications and status on the state of the intranet and database infrastructure and environment. This includes implementing, documenting, and monitoring patches, workarounds and updates.

The Assistant CIO (WCF) has responsibility for the security and operations of IT resources located at the BEP's Western Currency Facility (WCF).

Primary CSIRC responsibilities include:

- Facilitating communications between the WCF and Washington, D.C. facilities with respect to CSIRC activities;
- Identifying and allocating resources for protecting IT resources, assessing the impact of incidents and security measures on WCF operations; and
- Providing status on the state of the current IT infrastructure.

DATE July 31, 2002

The BEP CSIRC Management Team is responsible for ensuring that all incident response personnel, government or contractor have a background investigation and clearance commensurate with the classification level of the information with which they are working and viewing. The BEP CSIRC Management Team is also responsible for identifying and providing the necessary training for persons who fulfill CSIRC responsibilities.

2.2 BEP CSIRC Extended Team

The CSIRC Extended Team consists of individuals with functional responsibilities for, or expertise in, specialized operating systems, applications, and other non-standard information system resources exceeding the standard Bureau configuration; and those with responsibility for applying system updates and security fixes.

The BEP CSIRC Management Team may decide at any time to use the services of BEP CSIRC Extended Team members. Associate Directors and Office Chiefs are responsible for identifying persons within their respective areas having these capabilities prior to an incident. The BEP CSIRC Management Team may identify additional members of the Extended Team, as necessary. The names of the individuals identified, expertise of the specific system(s) or software application(s), office location, and office and home telephone numbers should be forwarded to the Manager, IT Security Division (ITSD). Some examples of Extended Team members are:

- Manager, Web Development Division (BEP Public Web and Intranet site, other BEP web servers, and related software applications)

- Manager, Enterprise Systems Division (IDMS, Oracle, SAP, BEPMIS, et. al.)

- Chief, Office of Production Engineering (Sun, Solaris, and DecAlpha platforms; Flo-Sys applications, et al)

- Chief, Office of Engraving (CGI platform; Unix OS; Fortuna application)

- Chief, Office of Stamp Production (Apple-Macintosh platform)

- Chief, Office of Financial Management (various financial applications)

- Chief, Office of Security (security systems)

- Chief, Office of Human Resources (HR Connect, etc)

- Chief, Office of External Relations, (Historical Resource Center Systems)

2.3 Incident Response Support Team

The Incident Response Support Team is an ad hoc team assembled to support the activities deemed necessary by BEP CSIRC Management. The team is typically staffed by the CIO Directorate, but may include additional individuals with specialized expertise in, or responsibilities for, information systems.

2.4 BEP CSIRC Relationships with Internal and External Organizations

Treasury CSIRC. The Treasury CSIRC provides alerts and advice to the BEP CSIRC Incident Coordinator regarding threats and vulnerabilities, incident response and investigation assistance. They coordinate department-wide security measures and incident reporting and analysis. Upon request, the Treasury CSIRC and Office of Information Systems Security will assist the BEP CSIRC with incident handling. Treasury support includes, but is not limited to, the following:

- Documenting the incident;
- Acting as a liaison between the Bureau and Treasury CSIRC;
- Ensuring Department incident handling guidelines and “best practices” are followed;
- Containing damage;
- Creating backups, if possible, of the affected systems;
- Resolving the problem; and
- Resuming business.

If an incident requires law enforcement investigation, the Treasury CSIRC will notify the Treasury Office of the Inspector General (IG), which will determine the appropriate law enforcement agency. Treasury will be the initial point of contact for the investigation. Law enforcement will coordinate with Treasury, the BEP Office of Security, and the BEP CSIRC regarding any computer forensics investigation and coordinate appropriate response, if necessary.

The Treasury CSIRC requires that all requests for outside assistance be made to, and coordinated by, the Treasury CSIRC.

Office of Security. The BEP CSIRC will notify the Chief, Office of Security immediately upon learning that law enforcement will or has become involved in any incident involving the BEP. The Chief, Office of Security is the primary BEP point of contact for coordination with law enforcement officials. The Chief, Office of Security will keep the Associate Director, CIO informed of the status.

Office of Management Control. The BEP CSIRC will notify the Chief, Office of Management Control if a situation arises that requires the involvement of the Treasury Office of the Inspector General (IG). The Chief,

DATE July 31, 2002

Office of Management Control will be the primary BEP point of contact for communication with the IG.

Office of External Relations. The Chief, Office of External Relations, is responsible for managing all communications with the public regarding the BEP (e.g., press releases, inquiries, etc.). The BEP CSIRC will refer all such requests for information to the Office of External Relations. The Associate Director (CIO) is the BEP CSIRC point of contact for the Office of External Relations.

BEP IT Disaster Recovery Teams. Authority to declare an IT disaster rests with the Associate Director (CIO) or his designee. Upon the declaration of a disaster, the CIO will direct the implementation of the BEP Disaster Recovery Plan, as appropriate. BEP CSIRC and Disaster Recovery Teams will work in partnership under the direction of the CIO.

3.0 CSIRC Services

The BEP CSIRC offers incident prevention, detection, response, and reporting services as described below.

3.1 Incident Prevention

Bulletins and Advisories. The ITSD will disseminate Treasury CSIRC and other applicable bulletins and advisories to the appropriate BEP CSIRC Management and Extended Team members. See Appendix B for a list of potential sources.

Time critical bulletins and advisories may be faxed, posted on the BEP Intranet, or sent through e-mail channels, in addition to alerting the appropriate BEP contact via phone or pager.

Treasury CSIRC e-mail bulletins and advisories will also be sent to the BEP CSIRC mailbox, accessible to ITSD and all BEP CSIRC management, to ensure the information is readily and widely available if designated monitors are unavailable.

Software Security Updates. The ITSD is responsible for initial identification and evaluation of security related updates for the BEP IT infrastructure. The Systems Support Division (SSD) is responsible for maintaining a complete and accurate inventory of hardware and software operating in the BEP environment. It is the responsibility of the Chief, Office of IT Operations (OITO), the Chief Technical Officer, the Chief, Systems Development Division (SDD), and all system administrators to ensure that software security patches, program upgrades, and service packs that have security implications are promptly implemented. If recommended patches are not implemented for operational or other reasons, the responsible administrator should prepare a justification for this omission. Information on

DATE July 31, 2002

patches, etc. applied or justifications for noncompliance must be provided to the Manager, IT Security Division.

Risk Mitigation Tracking and Reporting. The ITSD is responsible for establishing a vulnerability tracking system to track the assignment and status of actions to mitigate the risk of vulnerabilities. Vulnerabilities identified by vulnerability and risk assessments, bulletins and advisories, and other means will be entered in the system and referred by ITSD to the appropriate person for action. Referral recipients are required to acknowledge receipt of information, take appropriate steps to validate whether the cited vulnerabilities exist, and assess the recommended counter measures. They will report the status including specific actions taken, justification for any deviation from the recommended course of action, and issues that need further attention to the ITSD. System changes and updates will follow either routine or emergency configuration management procedures, as appropriate for the situation.

IT Security Advice and Risk Mitigation. The ITSD advises BEP users, system owners, administrators, and developers on technical and management issues related to IT security, vulnerabilities, threats, and risk mitigation.

Anti-Virus Protection. The ITSD has primary responsibility for managing the virus protection program and determining the configuration of anti-virus software. On a daily basis, ITSD will verify that the current virus definitions are installed on all systems listed in the system inventory (Asset Insite) and update virus definitions as necessary. ITSD has oversight responsibility for systems configuration related to anti-virus protection, e.g., e-mail configuration, attachment blocking, etc.

OITO and OSD ensure that all software is scanned prior to deployment. SSD is responsible for ensuring that all systems have current anti-virus protection installed and operational prior to deploying the systems, and that all installed systems are registered in the system inventory.

Periodic IT Security Training. The ITSD coordinates with the BEP Center for Excellence to develop and deliver role-based IT Security training mandated by the Computer Security Act of 1987, OMB Circular A-130, and the Government Information Security Act of 2001.

3.2 Incident Detection

The BEP CSIRC is responsible for ensuring that systems activity (e-mail volume, network traffic, firewall, and anti-virus logs) is actively monitored to identify anomalies that may indicate the occurrence of an IT security incident. The Manager, ITSD, will be notified when such anomalies are discovered.

DATE July 31, 2002

SSD will monitor network and e-mail activity. Operating system security logs, administrator access, configuration changes, anti-virus, firewall, intrusion detection, and other perimeter security, and incident detection tools are monitored by the ITSD. The ITSD has primary responsibility for identifying, implementing, and managing tools to aid the detection of IT security incidents.

Users are instructed to call the BEP IT Help Desk if they notice any unusual system activity or suspect an incident has occurred. The BEP IT Help Desk will also notify ITSD of when suspected incidents are reported, or when they suspect an incident may be occurring or has occurred.

3.3 Incident Response

The BEP CSIRC provides on-site and off-site support for authorized BEP IT resources, prioritizes and coordinates incident response activities, and determines the need for outside assistance and coordinates outside support through the Treasury CSIRC. Off-site support is typically provided via telephone or computer network.

If a situation exceeds the capacity of any BEP system support organization to assist BEP users or is likely to threaten the ability to conduct normal IT operation functions, the management of CSIRC activities is elevated to the BEP CSIRC Management Team.

The BEP CSIRC Management Team will determine if the incident will be handled in-house. If the incident exceeds the BEP's resources to address the incident, a request for onsite assistance will be forwarded to the Department's Office of Information Systems Security (OISS) through the Treasury CSIRC. The decision to request Treasury support rests solely with the BEP CSIRC Management Team. All requests for Departmental support of this nature by, or on behalf of, any BEP organization will be made through the BEP CSIRC. The BEP CSIRC shall coordinate all onsite visits related to the incident response, including receiving visitor requests to the Bureau with the exception of law enforcement agency visitors. These will be coordinated through the Office of Security.

The BEP CSIRC Management Team is responsible for establishing alternate Internet and e-mail communications capability for the use of designated BEP CSIRC personnel in the event it becomes necessary to disconnect from normal services.

3.4 Incident Tracking and Reporting

The Manager, ITSD, is responsible for establishing an incident tracking system to document all BEP IT security incidents. The incident tracking

DATE July 31, 2002

system will be used for follow-up reporting, trend analysis, evaluating the effectiveness of the CSIRC program, and to support legal action.

The Manager, ITSD, is also responsible for reporting incidents to the Treasury CSIRC according to Treasury guidelines. The Treasury CSIRC will report incidents to external agencies with which it has existing agreements, such as the Federal Computer Incident Response Center (FedCIRC) and the National Infrastructure Protection Center (NIPC). The Treasury CSIRC will forward Treasury trend analysis reports, lessons learned reports, and monthly Treasury CSIRC reports to OISS for distribution. All such reports will be written in such a way as to ensure the anonymity of the bureaus and personnel involved in the incidents.

4.0 Incident Response Guidelines

The BEP CSIRC has adopted Treasury CSIRC terminology and classification levels to facilitate clear communications and coordination among Treasury CSIRCs.

4.1 Incident Priority Levels

The BEP CSIRC will prioritize incidents using the five priority levels shown below. Priority is based on the impact to the BEP and Treasury Department's computing environments and can be expressed in terms of financial impact, impact to services and/or performance of our mission, impact to image or impact to trust by customers and the citizens of the United States. Incidents must be prioritized and handled accordingly. As additional information becomes available, the priority and criticality of the incident may change. Exhibit 1 provides a listing of the priority levels and a definition/description of each severity level.

Exhibit 1 – Incident Priority Levels

Priority Level	Definition
Priority One	Protect human life and safety. Human life always has precedence over all other considerations.
Priority Two	Protect classified data as regulated by government statutes and regulations.
Priority Three	Protect sensitive data, including proprietary, financial, law enforcement, scientific, and managerial. This includes CIP systems.
Priority Four	Prevent system damage (e.g., the loss or alteration of system files, damage to hard drives, etc.).

DATE July 31, 2002

Priority Five

Minimize disruption of computing resources. In many cases, it is better to shut down a system or disconnect from a network than to risk damage to data or systems.

4.2 The Five Phases of the Incident Response Process

While each incident is unique, the five-phase process described below provides a useful guideline for organizing incident response activities.

Identification. The BEP CSIRC will determine whether there may have been an error in configuration (network, software, application) or other action that may have led to the suspicious event. If a computer security incident has occurred, the BEP CSIRC will determine exactly what type and how many systems are affected.

It is critical for all those involved in the incident to take careful notes and to identify every piece of evidence. Access to the evidence shall be restricted and a complete chain of custody log shall be created. Details and knowledge of the incident shall be communicated on a “need-to-know” basis.

At its discretion, the BEP CSIRC may contact the Treasury CSIRC for assistance in determining whether the incident is a law enforcement issue.

Containment. Once an incident has been identified, the BEP CSIRC will determine the risk of continuing to operate the affected system(s). Efforts involve limiting the scope and magnitude of an incident. Because so many incidents observed currently involve malicious code, incidents can spread rapidly. This can cause massive destruction and loss of information. As soon as an incident is recognized, immediately begin working on containment.

It may be necessary to disconnect affected components from the network, disconnect the BEP network from the Internet, or shut down e-mail services.

If it is determined that the network has been attacked via an unauthorized external access, it is important not to alert the attacker until the system has been disconnected from the network. The CSIRC investigating party should avoid using the obvious methods such as “ping” and “ns lookup.” Once aware of being detected, the attacker may begin deleting files or erasing the file system to destroy evidence.

- A full backup shall be performed onto unused media and shall be safely stored for future use if law enforcement officials become involved.
- If possible, a second full backup will be made for use in comparison purposes.

DATE July 31, 2002

- All Bureau CSIRC members shall keep each other and the system owners advised of progress.
- The CSIRC shall gather router and system logs for review, as well as logs from neighboring systems.
- Passwords on the compromised systems and on all systems that interact with the compromised systems will be changed.
- Notify the system owner of potential unauthorized disclosure, system compromise, or unavailability.

Protecting BEP systems and data takes precedence over identifying the hacker.

Isolation. The BEP CSIRC will attempt to determine the symptoms and the cause of the incident. If an exact cause cannot be determined, a best guess based on the evidence at hand shall be made and included with the report. If the cause can be determined it will be quarantined and the most recent clean backup shall be utilized.

Recovery. Once a system has been restored, the CSIRC will test and verify that the restore operation was successful and that the system is safe and functional before bringing it back online to a production network. Every effort will be made not to restore back doors or malicious code. For example, if a root kit installation is suspected, the system shall be reformatted and the operating system shall be rebuilt, including all patches and fixes, prior to redeployment. Applications and data shall then be reloaded on the fresh operating system.

Follow-Up Assessment and Reporting. The BEP CSIRC will prepare a follow-up report for the Treasury CSIRC as soon as possible to ensure a full and accurate account of all details. Refer to the Treasury Computer Security Incident Response Procedures for detailed instructions and format. The BEP CSIRC will conduct a follow-up assessment to identify and document lessons learned and potential improvements to incident prevention and response policies and procedures.

DATE July 31, 2002

4.3 Generic Response Guidelines

Generic guidelines for responding to common types of incidents are detailed below.

Exhibit 2 – Generic Response Guidelines

Incident	Response
Malicious Logic	
Harmless virus	Disinfect infected files and disks. Attempt to determine source.
Destructive Virus	Disinfect infected files and disks. Attempt to determine source.
Trojan/Worm	Remove Trojan/Worm. Determine if any information was compromised and attempt to find IP/individual gathering information.
Mobile code	Determine damage. Disable mobile code (e.g., Java/Active X). Try to determine source.
Probes and Reconnaissance Scans	
	Probes and reconnaissance scans may indicate that the network is being targeted for an attack. All probes and scans should be reported to the Treasury CSIRC and all resources open to the Internet should be updated with the latest patches.
Unauthorized Access and Unsuccessful Attempts	
Unauthorized internal access or attempt	Determine if a user ID and password have been compromised. Change passwords. Ensure appropriate permissions are set and enforced.
Unauthorized external access or attempt	Determine user ID and password used. Change passwords. Unless otherwise directed by law enforcement, block access from outside if feasible.
Public disclosure of information	Determine and close source of disclosure.
Denial of Service Attacks	
Denial of service attack	Work with ISP to block the attacking IP address. Install any patches/fixes to the operating system.
E-mail bomb/E-mail attack	Coordinate defensive action with network operations.

DATE July 31, 2002

Incident	Response
Alteration/Compromise of Information	
Alteration of information	Establish what information may have been altered. Prioritize and then determine what had occurred.
Public disclosure of sensitive or classified information.	Same as above.
Adverse Mission Impact	
This category includes any type of incident not defined elsewhere. Response will vary with each incident.	
Classified System Incident	
Classified incidents must be reported as soon as possible. Ensure that the reporting method is secure.	
Loss or Theft	
Computer lost/stolen <u>with</u> classified or sensitive data	Report data that may have possibly been compromised, stolen, or lost.
Other	
This category includes events that may not obviously qualify as computer security incidents or necessitate a response, but may impact operations and could be interpreted as an incident. An unscheduled power outage, for example, may appear as a denial of service attack. In certain cases, these events should be reported to avoid unnecessary confusion.	

5.0 Incident Response Process

5.1 Initiating the Incident Response Process

Some CSIRC activities such as eradicating an isolated occurrence of a virus are handled by components of the CIO Directorate. Note that all potential computer security incidents must be promptly reported to the BEP CSIRC Incident Coordinator. The direction of these activities will be elevated to the BEP CSIRC Management Team when:

- CSIRC activities exceed the component’s capacity to handle; or

DATE July 31, 2002

- Appropriate Treasury or other Federal organizations communicate credible information concerning computer security threats or attacks; or
- The CIO or Deputy CIO identify situations as posing a serious threat to the Bureau's automated information resources.

Examples of some activities that could escalate into CSIRC situations are:

- Marked increase in trouble calls exceeding the capacity to handle in the routine manner, i.e., computer viruses, Trojan horses, and Internet worms; e-mail or printers are unavailable to user; computer hard drive crashes; software or applications fail.
- Sudden increase in calls from users indicating their computer is infected with malicious code; receipt of strange or unusual e-mails; data on computer or network missing, lost, or altered.
- E-mail servers inundated with e-mail; network response time slows down due to unexplained increase in activity; routers fail; computer hard drives crash; access to the BEP network, Intranet, or Internet is disrupted.

5.2 Escalation Levels

Incidents should be handled at the lowest escalation level that is capable of responding to the incident with as few resources as possible in order to reduce the total impact and to maintain tight control. However, as the impact or severity increases, the escalation levels below should be invoked by the CSIRC. At each escalation level, team members who will be needed at the next higher level of escalation are alerted to the incident so that they will be ready to respond if, and when, they are needed.

BEP CSIRC Management will consider several characteristics of the incident before escalating the response to a higher level. They are:

- How widespread is the incident?
- What is the impact to business operations?
- How difficult is it to contain the incident?
- How fast is the incident propagating?
- What is the estimated financial impact?
- Will this affect BEP's image negatively?
- Will protected information be compromised?

ESCALATION LEVEL 0

Normal Operations.

ITSD

1. Monitoring for alerts and software security patches from various sources.

DATE July 31, 2002

2. Monitoring system security logs, administrator access, configuration changes, anti-virus, firewall, intrusion detection, and other perimeter security, and incident detection tools.

SSD

1. Monitoring network and e-mail activity.

Customer Support Division (CSD)

1. Monitoring for reports of unusual system activity and suspected incidents.
2. Monitoring volume and type of calls

ESCALATION LEVEL 1

A possible threat has been discovered. (e.g., The BEP learns of a virus threat but it has not infected BEP systems.)

1. Notify the BEP Incident Coordinator (Manager, ITSD).

Incident Coordinator

1. Receive and track all reported potential threats.
2. Escalate Incident Response to Level 2 if a report is received indicating that the threat has manifested itself.
3. Determine CSIRC Team (CSIRC Management and Extended Teams) resources required to assess the threat.
4. Assemble CSIRC Team, if necessary.

BEP CSIRC Management Team

1. Determine initial defensive action required. (NOTE: At any point in the escalation process, the decision to disconnect from the Internet or discontinue e-mail services may be made by any member of the BEP CSIRC Management Team. A collaborative decision is preferable, however, the nature of the threat may require quick action. After such action, the Deputy CIO and CIO must be notified immediately. Treasury CSIRC must also be notified.)
2. Notify the appropriate IT organizations to initiate defensive action, if required.
3. If employee action required, notify the Help Desk and message employees of required action.
4. Notify the CSIRC Chair of the potential threat and actions taken to minimize risk.

DATE July 31, 2002

ESCALATION LEVEL 2

The threat has manifested itself. (e.g., There is a delay in the delivery of critical e-mail.)

Incident Coordinator

1. Notify Deputy CIO and CSIRC Team of the manifestation of the threat.
2. Receive status from the CSIRC Team.
3. Start a chronological log of events. NOTE: The chronological log will be used to provide information for reports to the Treasury CSIRC, follow-up assessments, and trend analysis. It will be used to support any follow-on disciplinary or legal action.
4. Contact the BEP users informing them of the incident if deemed appropriate by BEP CSIRC Management,
5. Contact the BEP users of any action they need to take as determined by the BEP CSIRC Management Team.

Deputy CIO

1. Assume responsibility for directing activities in regard to the incident,
2. Determine whether Escalation Level 2 is appropriate or escalate to level 3.
3. Determine when the risk has been mitigated to an acceptable level.

BEP CSIRC Management Team

1. Initiate the Incident Response Process. Determine best course of action.
2. Identify necessary resources.
3. Notify appropriate members of Extended Team and Incident Response Support Team, and provide direction for any action that is required.
4. Report actions taken and status to the Incident Response Coordinator.

Incident Response Support Team

1. Take action as determined by the BEP CSIRC Management Team.
2. Report actions taken to Incident Coordinator for the chronological log.

ESCALATION LEVEL 3

The threat has become widespread or has become a high severity level. (e.g., System availability is disrupted or confidential information has been compromised.)

DATE July 31, 2002

Deputy CIO

1. Determine when the risk has been mitigated to an acceptable level.
2. Evaluate, approve/disprove request for outside assistance.
3. Provide status to CIO and executive management, as appropriate.

Incident Response Coordinator

1. Continue to monitor all known sources for alerts looking for further information or actions to take to eliminate the threat.
2. Continue maintaining the Chronological Log of Event.
3. If the Deputy CIO determines that outside assistance is required, notify Treasury CSIRC and provide contact information for the BEP single point of contact, designated by the Deputy CIO.
4. If outside assistance is called in, make arrangements for building and system access.
5. Provide reports to Treasury CSIRC as required. Contact the BEP population as directed by the Deputy CIO.

BEP CSIRC Management Team

1. Continue reporting status to the Incident Response Coordinator for the chronological log of events.
2. Continue Incident Response Procedures.
3. Monitor effectiveness of actions taken and modify them as necessary.
4. Provide status to the Deputy CIO on effectiveness of actions taken and progress in eliminating the threat.
5. Determine need/recommend request for outside assistance.
6. Ensure that all needed information is being collected to support any disciplinary or legal action, or financial restitution.

Incident Response Support Team

1. Continue actions to eradicate the threat as directed by BEP CSIRC Management.
2. Continue to report actions taken, number of personnel, etc., to the Incident Response Coordinator for the chronological log.

6.0 Follow-up Assessment

The BEP CSIRC Management Team will assess the incident in terms of cause and identify any policies, procedures, controls or protections that could have

DATE July 31, 2002

prevented the incident or minimized impact. Review the escalation process and each of the five phases of the incident response process to identify opportunities for improvement. Determine if the appropriate resources (tools, information, personnel, skills, and outside support) were available when needed.

1. Document the following information:
 - Actions that could have prevented the incident
 - Estimate of damage/impact
 - Resources used
 - Action taken during the incident
 - Follow-on efforts needed to eliminate or mitigate the vulnerability
 - Policies or procedures that require updating
 - Additional resources needed
 - Additional training needed
 - Efforts taken to minimize liabilities or negative exposure
2. The chronological log and any system audit logs used in the incident response process.
3. Document lessons learned and modify the BEP CSIRC Procedures accordingly.
4. Perform a trend analysis.

7.0 Treasury CSIRC Reporting

The following events are computer security incidents and must be reported to the Treasury CSIRC:

- Malicious Code/Malicious Logic
- Probes and Reconnaissance Scans
- Unauthorized Access and Unsuccessful Attempts
- Denial of Service Attacks
- Alteration/Compromise of Information
- Adverse Site Mission Impact
- Classified System Incident
- Loss or Theft of Equipment

The BEP CSIRC will follow Treasury guidelines for reporting incidents to the Treasury CSIRC. Significant incidents¹ will be reported to the Treasury CSIRC as soon as possible, but not to exceed four hours from detection of an incident. Minor incidents² will be forwarded in a monthly summary report. If there are no incidents to

¹ Significant Incidents – Any information-security related incident that slows or prevents the use of a computer, a network or system for longer than 30 minutes, or impacts another bureau, agency or organization.

² Minor Incidents – Any information-security related incident that slows or inconveniences users in the use of a computer, a network or system, but does not prevent them from using information systems resources.

DATE July 31, 2002

report, a monthly summary report will be sent stating there were no incidents to report. The BEP CSIRC Incident Coordinator will report incidents on all BEP IT assets.

If, after their investigation, the BEP CSIRC determines the event is a security incident, the BEP CSIRC will report the incident to the Treasury CSIRC in accordance with TD P 71-10, Chapter VI, Section 5B, "Computer Security Incident Reporting" (draft).

If the BEP CSIRC determines the incident is internal³, the BEP CSIRC will report the incident to the appropriate internal authorities (e.g., the BEP Office of Security, BEP Office of Management Control, Treasury Office of the Inspector General (IG)) and will provide a close out report to the Treasury CSIRC. Detailed reporting procedures are described in the Treasury Computer Security Incident Response Capability (CSIRC) Procedures.

8.0 Updating BEP CSIRC Procedures

BEP CSIRC Management is responsible for the coordination and overall effectiveness of all CSIRC efforts. Therefore, updates to CSIRC procedures must be developed in collaboration with the full BEP CSIRC Management team. Members of the BEP CSIRC will provide written updates regarding their area of responsibility to the Manager, ITSD, who has primary responsibility for updating and distributing the BEP CSIRC Procedures manual.

³ An incident is determined to be internal if it is a bureau matter that has no impact on any other bureau, agency, or outside entity; and furthermore, the incident does not require any law enforcement investigation.

DATE July 31, 2002

Appendix A – Points of Contact

BEP CSIRC Management Team	Contact	Office Phone	E-Mail Address
Deputy CIO	Bob Scherer	(202) 874-3909	Robert.scherer@bep.treas.gov
BEP Incident Coordinator/ Manager, ITSD	Susan Polinsky	(202)874-3231	Susan.polinsky@bep.treas.gov
Chief, IT Operations	Shelia Lockley	(202) 874-2329	Shelia.lockley@bep.trea.gov
Chief Technical Officer	Phil Donehower	(202)927-1862	Phil.donehower@bep.treas.gov
Assistant CIO (WCF)	Dick Laird	(817)847-3883	Dick.laird@bep.treas.gov
Chief, Systems Development	Jeff Befumo	(202) 874-3717	Jeff.befumo@bep.treas.gov

Extended Team Area of Responsibility	Contact	Office Phone	E-Mail Address
BEPMIS, Public Sales, Enterprise Systems	Kathy Farhat-Sabet	(202) 874-3005	Kathy.farhatsabet@bep.treas.gov
In\$ite, Public Web Site	Carlos Moura	(202) 874-3006	Carlos.moura@bep.treas.gov

Incident Response Support	Contact	Office Phone	E-Mail Address
	Dan Perch	(202)874-3549	Daniel.perch@bep.treas.gov
	Ted Bamforth	(202)874-3208	Ted.Bamforth@bep.treas.gov
	Alan Haines	(202)874-3229	Alan.haines@bep.treas.gov
	Chris Masser	(202)874-3209	Chris.masser@bep.treas.gov
	Jim Riekse	(202)927-5008	James.riekse@bep.treas.gov

External Support	Contact Name	Phone Numbers
Treasury CSIRC	Carol Widmayer	(202) 622-1578
Treasury Office of Information Systems Security – Duty Desk		(202) 622-1110
Symantec – Gold Support for Norton AntiVirus 7.6	ID # 460014501	(800) 927-4017

After Hours or If Contact Can Not Be Reached	Phone Numbers
Help Desk (Washington D. C.)	(202) 874-3010
Brenda Veal-Munoz (WCF)	(817) 528-1397

DATE July 31, 2002

Appendix B – Sources of Incident Response and Advisory Information

Source
Computer Emergency Response Team Coordination Center (CERT/CC) http://www.cert.org
NIST Vulnerability and Threat Portal http://icat.nist.gov/vt_portal.cfm
Federal Computer Incident Response Center (FEDCIRC) http://www.fedcirc.gov
Federal Computer Incident Response Center (FEDCIRC) Patch Authentication and Dissemination Capability (PATCHES) http://www.fedcirc.gov and select "Patches"
Microsoft Security Advisory —Discusses Security vulnerabilities in all Microsoft products and has patches available. http://www.microsoft.com/security/default.asp
Symantic Anti-Virus Support http://www.symantec.com