

DATE June 27, 2001

---

**GATEWAY/FIREWALL POLICY**

---

**1. Purpose and Scope.** This Circular establishes policy guidance for implementing Internet Protocol (IP) connectivity from Bureau networks to the Internet, intranets and other networks. The Circular has applicability to all communications within the Bureau, between the Bureau and Fort Worth, and between the Bureau and external sites. This policy does not affect user guidelines except in requiring that external communications are directed only through the Bureau firewall.

**2. Background.** The purpose of a firewall is to protect internal information systems from external attacks. An inter-connected environment is desirable for conducting Bureau and Government business, but is also susceptible to various forms of attack, resulting in loss of service or compromise of information. A risk to one system becomes a risk to many systems and a firewall forms part of a comprehensive security strategy to counter external threats.

**3. References.**

“Gateways/Firewalls,” Department of the Treasury Security Manual TD P 71-10, VI. 4.C.4-S., January 13, 1999.

“Technical Security Standard (TSS) 001: Gateways/Firewalls,” Department of the Treasury Security Manual TD P 71-10, VI.4.C.4, January 13, 1999.

“Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls,” National Institute of Standards and Technology (NIST) Special Publication SP 800-10, December 1994.

“Firewalls,” Information Assurance Technical Framework (IATF) version 3.0, National Security Agency, September 2000.

“Firewall Technical Security Standard,” BEP Technical Standard, Associate Director (CIO).

“Certification and Accreditation of BEP Systems and Applications,” BEP Circular No. (in draft, pending approval).

**4. Policy.** It is the policy of the Bureau of Engraving and Printing that:

a. All connections between Bureau networks or networked devices (including local area networks, e-mail services, In\$ite, or dedicated computers) and external sources (such

DATE June 27, 2001

as remote service to Bureau computing devices, the Internet, and Treasury or other extranets) shall be centrally managed. This requirement for central control and security review also applies to dial-up service, including modems and public telephone service, even though the service may not pass through a Bureau firewall.

b. Any direct connection to the Internet or an extranet or any e-mail service must pass through the Bureau firewall. Any incoming services, including dial-up access to the LAN or mainframe, shall also pass through the Bureau firewall.

c. The firewall will be configured so as to exclude any services or types of transmission except those which are explicitly permitted. For example, only those Transport Control Protocol (TCP) or User Datagram Protocol (UDP) services which are specifically permitted shall be allowed.

d. Bureau laptop computers which are operated in a remote configuration with connectivity to the Bureau LAN or any computer with independent connectivity to the Internet shall have a firewall installed, which will be configured to meet the requirements for laptop computers in the Bureau "Firewall Technical Security Standard."

e. The Bureau firewall will be treated as a general support system and will be certified and accredited in accordance with the requirements contained in the Bureau Circular, "Certification and Accreditation of BEP Systems and Applications."

f. The Bureau firewall will log incoming and outgoing traffic and will have the capability for identifying suspicious activities. These audit files will be maintained for a prescribed period and may be used in investigations or for other official purposes.

## **5. Responsibilities.**

a. The Manager, Systems Support Division shall:

(1) designate the system administrator and an alternate system administrator for the Bureau firewall;

(2) configure the Bureau firewall according to the applicable Firewall Technical Security Standard and shall document, with justification, any changes to the configuration. All configuration changes shall be coordinated with the Information Technology Security Division (ITSD) prior to implementation;

(3) provide mechanisms for reduction of audit logs and shall report suspicious activity to ITSD;

(4) enable log alarm functions and report alarms immediately to ITSD;

(5) maintain firewall operating capability, including developing contingency procedures for use when firewall is disabled or compromised; and

(6) develop a process for exceptions and waivers to firewall configuration or firewall standards that includes, as a minimum:

**CIRCULAR**

No. 10-08.24

DATE June 27, 2001

(a) a description of the exception or waiver and the rationale, including a business case, if applicable;

(b) an assessment of risk associated with granting the exception/waiver;

(c) a presentation of actions that could mitigate risk; and

(d) approval of ITSD.

b. The Manager, Information Technology Security Division shall:

(1) issue password and other administrator access and authorization for the Bureau firewall, and shall periodically monitor access and system utilization by the administrator;

(2) review and evaluate firewall configuration and changes to that configuration;

(3) identify patches and upgrades for system bugs or vulnerabilities;

(4) appoint a backup firewall system administrator;

(5) periodically audit the firewall and shall review system audit logs on other occasions as necessary;

(6) shall coordinate with the Manager, Systems Support Division, in certifying and accrediting the Bureau firewall and in making any subsequent hardware or software modifications;

(7) approve firewall software;

(8) review and approve any firewall contingency plans to ensure backup alternatives do not compromise security or privacy; and

(9) review and evaluate business cases or other justification for applications or services which require exceptions or amendments to firewall policy.

c. The Chief, Office of Systems Development shall coordinate access requirements for new web, database, or intranet applications to ensure that services required to support the Bureau business through the firewall are within the approved security framework or that a business case has been developed and approved by the CIO for exceptions.

d. Bureau users shall not attempt to circumvent the Bureau firewall or to disable the connectivity of computers through the firewall.

**6. Office of Primary Responsibility.** Associate Director (Chief Information Officer).

**<SIGNED>**

Ronald W. Falter  
Associate Director (CIO)

Distribution: CIO Directorate  
Director  
Deputy Director  
Associate Directors  
Office Chiefs