PERIMETER PROTECTION

ISSP-24-0410

1. **SUBJECT:** Adequate protection must be implemented to protect OPIC information resources from intruders and service disruption.
2. **SCOPE:** This policy applies to all external entry points into OPIC information systems, including but not limited to Internet connection(s) and communication links to other agencies.
3. **DESCRIPTION:** Any connectivity to systems or organizations outside of OPIC provides an opening for unauthorized personnel to access or tamper with OPIC information resources. Such threats range from intruders breaking into OPIC's network to steal or alter data to service disruptions propagated from other systems. OPIC must implement firewalls, intrusion detection systems, and other precautions to prevent, detect, and resolve incidents arising from these threats.
4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will use firewalls and other security devices to provide filtering and auditing of traffic on all external communication links.

   (1) OPIC will use a Firewall and an Intrusion Detection System (IDS) on all Internet connections.

   (2) Routers with firewall features (e.g., packet filtering, logging) may be used for connections to other federal agencies.

   (3) Traffic into OPICNET from external systems must be filtered to allow only the minimum access required to meet OPIC business requirements.

   (4) Firewalls and IDS systems should be configured and administered in accordance with government and industry best practices, including but not limited to:

   - The default filters must specify that all access into OPICNET be denied unless specifically permitted.
   - Each firewall, IDS, and other perimeter security device must be actively monitored, and periodically audited, for threats to OPICNET.
   - Firewall and IDS equipment provide real-time notifications or alerts to administrators upon security events.
   - Upon a system failure, firewalls will default to a "Deny All" configuration until reset by an administrator.
   - When feasible, Firewall services should run on a dedicated system with all other services disabled.
   - Source routing will be disabled on all firewalls and external routers.

- The firewall will not accept traffic on its external interfaces that appears to be coming from internal network addresses.
- The firewall will be configured to implement transparency for all outbound services.
- The administrator(s) will review the network security policy and maintenance procedures on a regular basis (every three months minimum). Where requirements for network connections and services have changed, the security policy will be updated and approved.
- The firewall implementation (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be locked up so that the media is only accessible to the appropriate personnel.
- Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall software must be done by a firewall administrator(s) and requires the formal approval of the ISSO.
- The firewall administrator(s) must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.
- All services and traffic to be authorized across the firewall implementation must be well documented. Documented will be the business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.
- The firewall is to run as a DNS server in order to provide public/Internet addresses to clients. The firewall will be configured to hide information about the network so that internal host data are not advertised to the outside world.
- Routing by the firewall will be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

(b) Any OPIC systems or services that are to be publicly available on the Internet must adhere to the following rules:

(1) These systems must be placed in a protected DMZ.

(2) No sensitive data is to be stored on systems located in the DMZ. All sensitive data must be located inside the firewall.

(3) Access from the Internet to these systems must not make sensitive information or information systems vulnerable to compromise.

(c) The details of OPIC's internal network should not be visible or accessible from outside the firewall.

(d) Proxy Servers:

(1) All outbound connections to the Internet will be performed through a Proxy server. A proxy server provides a number of security enhancements by concentrating services through a specific host to allow monitoring, hiding of internal structure, etc.

(2) Because this funneling of services creates an attractive target for a potential intruder, additional measures should be deployed to protect the proxy server.

(e) Any remote access into OPICNET through the firewall (e.g., telecommuting applications) must utilize strong authentication and encryption, and adhere to OPIC remote access policies and procedures.

(f) All perimeter equipment must be documented in accordance with OPIC information system documentation procedures.

(g) Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to OPIC change control procedures.

(h) Information regarding the configuration of firewall and other perimeter protections is considered confidential and is to be treated as Sensitive But Unclassified (SBU) data.

(i) All hardware and software deployed on the perimeter must adhere to OPIC system security policies and procedures, including the disabling of all unnecessary services.

(j) All security related events on perimeter equipment, as well as access to OPICNET via this equipment, must be logged and audited in accordance with OPIC's Audit Trail policies and procedures.

(k) The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. COTRs are responsible for third party compliance with this policy.

(l) Employees will access the Internet only through OPIC-approved Internet access points. Any form of communication to or from workstations outside the internal (trusted) network is strictly prohibited without authorization. This includes modems, leased lines to other networks, etc.

(m) Network Trust Relationships:

(1) All connections between OPICNET and external networks (such as those of other agencies) must be approved IRM.

(2) Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.

(3) An interconnection security agreement will be developed and signed by OPIC and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.

(4) All connections to approved external networks will pass through OPIC approved firewalls.

(5) Information Owners will validate the need for all such connections on an annual basis.

(6) When notified by an Information Owner that the need for connection to a particular network is no longer valid, all accounts and parameters related to the connection should be deleted within 5 working days.

(n) The use of any of the following services on DMZ systems and perimeter systems, and the permitting of these services into OPICNET from external sources, must be approved by the ISSO: HTTP, FTP, Telnet, Finger, WHOIS, Gopher, SSL, SQL, RSH, NNTP, TN3270, Rlogin, POP3, and streaming media.

(o) Multiple layers of perimeter protections should be used to create Defense in Depth.

(p) OPIC should adhere to NIST guidance as set forth in Special Publications 800-41, Guidelines on Firewalls and Firewall Policy, 800-31, Intrusion Detection Systems; and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that the resources they own comply with the guidelines specified in this policy, including but not limited to:

(1) Obtaining appropriate authorizations and agreements for:

- Any external connections required by their systems.
- Any systems/services they own that are placed outside an OPIC firewall.
- External Access through the OPIC perimeter into their systems that are located inside OPICNET.

(2) Applying appropriate perimeter protections to any externally accessible resources that they own.

(3) Configuring any perimeter resources that they own (including security devices) in accordance with the above-specified guidance.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with the implementation and management of perimeter protections and system configurations to comply with this policy.

(2) Assisting the ISSO with auditing of perimeter protections and system configurations.

(3) Immediately reporting any perimeter breaches or potential vulnerabilities to the ISSO.

(c) Information Users are responsible for accessing the Internet and other external systems only through OPIC approved connections and in accordance with OPIC security procedures.

(d) Supervisors are responsible for ensuring that their employees understand and comply with this policy.

(e) The Information Systems Security Officer (ISSO) is responsible for:

(1) Auditing OPIC information resources for compliance with this policy.

(2) Reviewing and approving access, connectivity, and services provided between OPICNET and external systems.

(3) Providing guidance to Information Owners and Custodians regarding perimeter security.

6. DEFINITIONS:

(a) DMZ (De-militarized Zone) - Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within OPICNET or to provide services to external parties.

(b) Encryption – The process of transforming readable text into unreadable text (cipher text) for the purpose of security or privacy. Data is encoded to prevent unauthorized access.

(c) Firewall - A logical barrier guarding a private network by analyzing the data leaving and entering. It stops users or processes from going beyond a certain point in a network unless they have first passed some security test.

(d) Intrusion - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource through unauthorized access or penetration of an information resource.

(e) Intrusion Detection System (IDS) – A system that analyzes network traffic to detect anomalies and provide alerts regarding possible intrusions.

(f) Perimeter – The boundary between OPIC owned/operated information resources and those under the control of another party.

(g) Perimeter Equipment – Any devices or servers which form part of the perimeter (e.g., perimeter router), are deployed to protect the perimeter (e.g., firewall), or which reside on the perimeter (e.g., DMZ web servers).

(h) Proxy Server - A system that acts on behalf of a user or process. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

(i) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.

7. **ENFORCEMENT:** Violation of this policy could result in loss or limitations on use of information resources, as well as disciplinary and/or legal action, including termination of employment or referral for criminal prosecution.
8. **POINT OF CONTACT:** OPIC Information Systems Security Officer (ISSO)
9. **ATTACHMENTS:** None
10. **AUTHORITY:**

    (a) OPIC Directive 00-01, Information Systems Security Program.

    (b) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

    (c) OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

    (d) NIST Special Publication 800-41, Guidelines on Firewalls and Firewall Policy.

    (e) NIST Special Publication 800-31, Intrusion Detection Systems.

    (f) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.
11. **LOCATION:** TBD
12. **EFFECTIVE DATE:** October 22, 2004
13. **REVISION HISTORY:** None
14. **REVIEW SCHEDULE:** This policy should be reviewed and updated annually.