INCIDENT RESPONSE

ISSP-06-0410

1. **SUBJECT:** Agency must be able to respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

2. **SCOPE:** This policy applies to all OPIC information users, owners, and custodians.

3. **DESCRIPTION:** The Federal Information Security Management Act (FISMA), and OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems require all organizations to have an incident response capability and to share information concerning common vulnerabilities and threats.

   A formally documented and clearly understood incident response process will make it possible for OPIC to respond quickly and effectively to situations that might compromise the agency's information resources.

4. **PROCEDURES & GUIDELINES:**

   (a) All reported security incidents will be responded to quickly and in adherence to OPIC InfoSec incident handling procedures.

   (b) OPIC will establish Information Security Incident Response procedures to address computer security incidents, including theft, misuse of data, intrusions, hostile probes, and malicious software.

   (c) When an incident occurs, the information user or their supervisor must provide a verbal report to the ISSO within one working day after the incident. Critical incidents must be reported immediately.

   (d) A written preliminary report must be completed within two working days using OPIC's incident reporting form. This report is to be completed by the individual handling the incident. Within five working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty days, a weekly status report must be submitted to the ISSO.

   (e) Priority in incident handling should be given to preventing further damage to OPIC information resources.

   (f) Should a breech be serious enough to warrant prosecution, law enforcement will need to demonstrate a chain of custody and provide records of what actions were taken. Therefore, a log must be kept of all the actions taken, including triage steps and other regular or routine work performed on the affected systems. This log should be separate from normal system logs, since it may be used as evidence.

   (g) OPIC will enter into and maintain a cooperative agreement with the Department of Homeland Security/US-CERT to facilitate share incident information and provide assistance with incident resolution.

(h) OPIC will adhere to NIST guidance as set forth in Special Publication 800-61, Computer Security Incident Handling Guide, and subsequent publications, as well as relevant guidance from US-CERT.

5. ROLES & RESPONSIBILITIES:

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

(1) Preparing policy guidelines for establishing and implementing a computer security incident response capability

(2) Developing incident response procedures

(3) Working with law enforcement, the users, information owners, and system administrators to formulate and implement a response plan

(4) Notifying the information owners and OPIC management of significant incidents and the response plan

(5) Ensuring that all incidents and resolution activities are fully documented and tracked

(6) Providing information on incidents to the Department of Homeland Security/US-CERT.

(b) Information Users are responsible for:

(1) Performing the following if they suspect a security incident may have occurred:

- Understanding and complying with OPIC incident handling procedures
- Documenting all relevant information about the suspected incident
- Sharing the suspicion and information with their manager and/or the ISSO
- Fully cooperating with and assisting the ISSO, system administrators, and other designated personnel with resolution of the incident as requested

(c) Supervisors are responsible for:

(1) Ensuring that their employees understand OPIC incident response policy and procedures,

(2) Contacting the ISSO within one working day after the incident,

(3) Providing incident-related information to the ISSO when requested

(d) Information Owners are responsible for:

(1) Ensuring that incident response procedures are in place for their resources

(2) Informing OPIC management of significant incidents (major compromise of data, denial of service).

(3) Providing follow up to ensure that incidents have been resolved

(e) Information Custodians are responsible for:

(1) Assisting with evaluation and mitigation of the incident

(2) Working with the ISSO, system owner, and/or users, to formulate and implement a response plan,

(3) Documenting and reporting steps taken to handle the incident to the ISSO

6. DEFINITIONS:

(a) Security Incident - Any activity that is a threat to the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

(b) Critical Incident – An incident that will result in a severe impact to OPIC resources if not addressed quickly.

7. ENFORCEMENT: Anyone who violates this policy is subject to disciplinary action, up to and including termination of employment.

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) Information Technology Systems.

(e) Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

(f) NIST Special Publication 800-61, Computer Security Incident Handling Guide.

(g) 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.