INCIDENT REPORTING

ISSP-05-0410

1. **SUBJECT:** All OPIC information users are required to report any suspected information security incidents in accordance with OPIC incident reporting procedures.
2. **SCOPE:** This policy applies to all users of OPIC information resources.
3. **DESCRIPTION:** Maintaining the security of OPIC information resources requires cooperation and participation from everyone. It is important that all information users maintain vigilance regarding information security, and immediately report any suspected incidents in order to minimize potential damage to OPIC.

   OPIC's security incident reporting policy and procedures enable OPIC to quickly and efficiently recover from security incidents; respond in a systematic manner to incidents and carry out all the necessary steps to correctly handle an incident; prevent or minimize disruption of critical computing services; and minimize loss or theft of sensitive or mission-critical information.

4. **PROCEDURES & GUIDELINES:**

   (a) All suspected security incidents must be reported immediately to the ISSO.

      (1) Incidents include, but are not limited to:

      - Suspected violations of any OPIC information security policies.
      - Loss or theft of laptops, mobile devices (such as PDAs), security tokens, or other items that may provide access to OPIC information resources.
      - Attempts by unauthorized external personnel to gain access to OPIC information or systems.
      - Accidental disclosure, modification, or destruction of information.

   (b) All reported incidents will be handled in accordance with OPIC Incident Handling policies and procedures.

      (1) An OPIC incident report form must be completed and submitted for each incident.

   (a) OPIC will adhere to NIST guidance as set forth in Special Publication 800-61, Computer Security Incident Handling Guide, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

   (a) Information Users are responsible for reporting suspected incidents to the ISSO or information owner immediately, using OPIC incident reporting procedures.

   (b) Supervisors are responsible for ensuring that their employees understand and adhere to incident reporting policies and procedures, and for ensuring that security incidents are reported as quickly as possible.

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

(1) Developing and maintaining incident reporting and handling procedures.

(2) Researching, documenting, resolving and tracking reported incidents.

(3) Reporting incidents to upper management and appropriate external entities.

(4) Determining if incident follow-up is needed.

(d) Information Custodians are responsible for:

(1) Reporting any incidents they encounter to the ISSO.

(2) Researching and resolving incidents within their administrative domain.

(3) Providing documentation of incidents and steps taken to resolve them to the ISSO.

(4) Fully cooperating with and assisting the ISSO with incident handling as requested.

(e) System Administrators are responsible for assisting the ISSO with researching, documenting, resolving and tracking reported incidents.

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.

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

(d) NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems.

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

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

14. REVIEW SCHEDULE: This policy should be reviewed and updated annually.