CERTIFICATION AND ACCREDITATION

ISSP-08-0410

1. **SUBJECT:** Each of OPIC's major information systems will be certified and accredited every 3 years or upon each significant change to the system (whichever comes first).
2. **SCOPE:** This policy applies to all major information systems at OPIC.
3. **DESCRIPTION:** The purpose of Certification and Accreditation (C&A) is to ensure that information systems have adequate security commensurate with the level of risk. To this end, C&A is the formalized process used to assess the risks and security requirements of each system, and to determine whether the system's security needs are being met.

   The Federal Information Security Management Act (FISMA) requires OPIC to perform C&A of its information systems. For each system, this process must be completed either every 3 years or when there is a change that affects the system's security posture.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC shall assign a senior executive (preferably the Chief Information Officer) to act as the Designated Approving Authority (DAA) to accredit OPIC information systems.

   (b) Certification:

   (1) OPIC shall implement a Certification program to test and evaluate technical and non-technical IT security features and other safeguards used by OPIC systems, in support of the Accreditation process.

   (2) Certification shall not only address software and hardware security safeguards, but also procedures, physical protections, and personnel security measures.

   (3) Security Testing & Evaluation (ST&E) will be performed during the Certification process to evaluate the effectiveness of security measures implemented for the system.

   (4) The following minimum requirements must be met for a system to be certified:

   - The system must be thoroughly documented.
   - A system security plan must be developed and approved.
   - An ST&E of the system must be completed.
   - A risk assessment must be conducted.
   - Standard operating procedures must be developed for the system.

- The system must meet all applicable legal requirements and OPIC policies.
- A contingency plan must exist for the system.

(c) Accreditation:

(1) OPIC shall implement an Accreditation process used for obtaining official management authorization for the operation of an IT resource.

(2) Accreditation will be in the form of a formal declaration by the DAA that an IT resource is approved to operate in a particular security mode using a prescribed set of safeguards.

(3) The Accreditation determination shall be based on findings, facts, and support documents produced during the Certification process, as well as other management considerations.

(4) An Accreditation statement, which affixes security responsibility with the accrediting authority (DAA), will be used to certify that proper attention has been afforded to the security of the IT resource.

(5) The statement shall address the residual risks associated with the respective system or network, subsequent to the implementation of countermeasures applied during the system test and evaluation.

(d) Certification and Accreditation statements shall be completed for all major applications and general support systems.

(e) Information Owners will review Certification and Accreditation statements before they are signed by the DAA.

(f) An Interim Authority to Operate (IATO) may be issued in those cases in which systems must be implemented expeditiously, but the IATO should last no longer than 6 months and should only be granted if it does not pose a significant risk to OPIC information resources.

(g) Existing operational systems that have not been certified and accredited within the last 3 years shall undergo Certification and Accreditation within 1 year of the issue date of this order.

(h) All new OPIC IT systems will be certified and accredited prior to being allowed into operation.

(i) All systems will be recertified and reaccredited at least every three years or when there is a significant change to the security posture of the system, whichever is earlier.

(j) OPIC will adhere to NIST Certification and Accreditation guidance as set forth in Special Publication 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for:

(1) Ensuring that C&A requirements are met for any major information systems they own, including developing a security plan for each system.

(2) Notifying the ISSO when there is a significant change to the security posture of a major information system.

(3) Reviewing C&A statements before they are signed by the DAA.

(4) Addressing any remedial action that must be taken subsequent to the ST&E.

(b) Information Custodians are responsible for:

(1) Assisting information owners in ensuring that major information systems are certified.

(2) Assisting the ISSO with conducting ST&E.

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

(1) Developing and communicating OPIC's C&A procedures

(2) Ensuring that major information systems have been certified and accredited

(3) Assisting with the development of system security plans.

(4) Conducting ST&Es of major information systems.

(5) Forwarding C&A statements to the DAA for review.

(d) The Designated Approving Authority (DAA) is responsible for:

(1) Acting as the authorizing official for Accreditation of IT resources.

(2) Completing and signing C&A statements and forwarding them to the ISSO.

(3) Granting IATOs and developing timeframes in which remedial actions must be taken.

6. DEFINITIONS:

(a) Accreditation – A risk-based decision that determines whether an IT system should be allowed to operate under a particular security configuration. Accreditation is based on the facts, plans, and schedules developed during Certification.

(b) Certification – An assessment of the security controls of an information system.

(c) Designated Approving Authority (DAA) – The senior management official or executive with the authority to approve the operation of an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

(d) General Support Systems – An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people, and provides support for a variety of users and applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

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 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems,

    (e) 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.