ENCRYPTION

ISSP-15-0410

1. **SUBJECT:** OPIC will use proven, government-approved encryption technologies to protect sensitive information.

2. **SCOPE:** This policy applies to the use of encryption for protecting unclassified OPIC information during storage or transmission.

3. **DESCRIPTION:** The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively. Additionally, this policy provides direction to ensure that Federal regulations are followed, and recognizes the legal authority for the dissemination and use of encryption technologies outside of the United States.

4. **PROCEDURES & GUIDELINES:**

   (a) The use of encryption to protect sensitive data, both in storage and in transmission, is highly encouraged.

   (b) Only government-approved encryption techniques and devices may be used.

      (1) All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.

      (2) Digital certificates used or issued by OPIC will comply with the Federal Public Key Infrastructure.

   (c) The use of proprietary encryption algorithms is not allowed for any purpose, unless reviewed by qualified experts outside of the vendor in question and approved by the ISSO.

   (d) OPIC will obey all regulations regarding restrictions on export of encryption technologies.

   (e) OPIC will have documented and implemented procedures for managing encryption keys, in order to ensure that these keys are protected from unauthorized disclosure, destruction, or misuse.

   (f) Any use of digital certificates to provide non-repudiation must be approved by the ISSO and Legal Affairs.

   (g) OPIC will adhere to NIST guidance as set forth in Special Publications 800-21, Guide for Implementing Cryptography in the Federal Government; 800-57, Recommendation on Key Management; 800-38, Recommendations for Block Cipher Modes of Operation; 800-32, Introduction to Public Key Technology and Federal PKI Infrastructure; 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication; 800-15, Minimum Interoperability Specification for PKI Components; and other publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that the use of encryption by, or protection of, systems that they own are compliant with the terms of this policy and all applicable federal standards.

(b) Information Custodians are responsible for assisting information owners with implementing and managing encryption technologies compliant with this policy.

(c) The ISSO is responsible for providing guidance on the use of encryption technologies and auditing OPIC users and systems for compliance with this policy.

6. DEFINITIONS:

(a) Digital Certificate - The electronic equivalent of an ID card. A digital certificate, which may contain a users name and other information, is issued by a certification authority (CA), which also keeps track of digital certificates that have been revoked.

(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) Encryption Key - A secret password or bit string used to control the encryption process.

(d) Non-repudiation - Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.

(e) Proprietary Encryption - An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

(f) Public Key Cryptography - A coding system in which encryption and decryption are done with public and private encryption keys, allowing users who don't know each other to send secure or verifiable messages.

(g) Public Key Infrastructure (PKI) - A system for securely exchanging information that includes a method for publishing the public keys used in public key cryptography and for keeping track of keys that are no longer valid.

(h) Sensitive Data – Any data that is categorized as “sensitive” under OPIC’s information resource classification policy and framework.

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) Computer Security Act of 1987 (Public Law 100-235).

(e) Federal Information Processing Standard (FIPS) 140-2, Security requirements for Cryptographic Modules.

(f) Federal Information Processing Standard (FIPS) 197, Advanced Encryption Standard.

(g) NIST Special Publication 800-21, Guide for Implementing Cryptography in the Federal Government.

(h) NIST Special Publication 800-57, Recommendation on Key Management .

(i) NIST Special Publication 800-38, Recommendations for Block Cipher Modes of Operation; 800-32.

(j) NIST Special Publication Introduction to Public Key Technology and Federal PKI Infrastructure.

(k) NIST Special Publication 800-25, Federal Agency Use of Public Key Technology for Digital Signatures and Authentication.

(l) NIST Special Publication 800-15, Minimum Interoperability Specification for PKI Components.

(m) 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.