OVERSEAS PRIVATE INVESTMENT CORPORATION

1. **TITLE:** Information Systems Security Program

2. **PURPOSE:** OPIC's Information Systems Security Program (ISSP) establishes policies and procedures, and designates responsibilities and authorities for ensuring an adequate level of information security for all unclassified information collected, created, processed, transmitted, stored, or disseminated on the agency's information systems.

3. **SCOPE:** This directive applies to all OPIC Information Users, including employees, vendors and visitors, and anyone who uses or has access to any OPIC information resources.

4. **DEFINITIONS:**

   4.1. Employees, as used in this directive, refers to individuals hired in the competitive or excepted civil service, including students and temporary employees, as well as personal services contractors, industrial contractors, consultants and experts hired on contract.

   4.2. Information Users are individuals who use or have access to OPIC's information resources, including employees, vendors, and visitors.

   4.3. Information Owners are the individuals ultimately responsible for information resources, and are generally Departmental Vice Presidents, or designated senior managers. The initial owner is the individual who creates, or initiates the creation or storage of, information. Once information is created or stored, the individual's respective OPIC business unit becomes the Owner, with the Departmental Vice President of that unit taking official responsibility.

   4.4. Information Custodians are individuals (*e.g.*, IRM staff) who maintain or administer information resources on behalf of Information Owners.

   4.5. Supervisors are OPIC employees who have formal supervisory responsibility for employees, contractors, or other information users. This includes managers, COTRs, visitor escorts, and other supervisory personnel.

   4.6. Information Resources are equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

   4.7. A security incident is any activity that is a threat to the availability, integrity, or confidentiality of OPIC's information resources, or any action that is in violation of this directive or its implementing administrative orders.

5. RESPONSIBILITIES:

5.1. All OPIC information users share in the responsibility of protecting the organization's information resources and adhering to the agency's policies on their usage.

5.2. The Chief Information Officer (CIO) monitors, evaluates, and reports the status of information security within the Corporation to the President and CEO. The CIO also ensures that the ISSP aligns with OPIC's business objectives, and that information technology decision-making includes an analysis of the risks involved.

5.3. The Director of Technical Services (DTS) oversees the development and operation of the ISSP, and ensures integration of the program with other IRM initiatives, procedures, and strategic plans. The DTS also acts as liaison with senior management regarding approval and status of OPIC information security policies and practices.

5.4. The Information Systems Security Officer (ISSO) develops, implements and maintains an ISSP within OPIC. The ISSO ensures the confidentiality, integrity and availability of OPIC information resources via formal policies, awareness training, compliance monitoring and security controls. The ISSO assesses risk, develops policies and procedures, provides security guidance, conducts compliance reviews, and assures investigation of information security incidents. The ISSO may establish working groups regarding security matters.

5.5. Information Owners - While the day-to-day function of administering and protecting data is the responsibility of an Information Custodian, Information Owners have final corporate responsibility for their information resources. Information Owners are responsible for:

5.5.1. Categorizing their business processes, information, and systems according to a standard classification framework developed by the ISSO;

5.5.2. Ensuring that the information resources they own are adequately protected based on their classification and the level of risk;

5.5.3. Authorizing access to information resources based on a need-to-know;

5.5.4. Communicating procedures for securely handling information resources to Information Users; and

5.5.5. Delegating stewardship of information resources to an Information Custodian.

5.6. Information Users must be known to and authorized by Information Owners. Information Users are responsible for:

5.6.1. Understanding and complying with OPIC information policies and guidelines (including the *Information Security Handbook)*; and

5.6.2. Exercising due diligence in protecting information in their possession from unauthorized access, alteration, destruction, or improper usage.

5.7. Information Custodians are responsible for:

5.7.1. Safeguarding the information in their possession;

5.7.2. Assisting Information Owners with the management of information resources; and

5.7.3. Adhering to policies and guidelines for information and system management.

5.8. Supervisors are responsible for ensuring that their employees understand their information security responsibilities, and for taking disciplinary actions related to employee violations of OPIC ISSP policies, procedures, and guidelines.

6. TEXT:

6.1. The OPIC ISSP comprises a set of information security policies, as well as standards, guidelines, and procedures for their implementation. These policies and procedures will be communicated to Information Users via administrative orders (*i.e., Information Systems Security Program Handbook* and other issuances), which are incorporated into this directive by reference.

6.2. The ISSO will educate employees about information security, and the policies and procedures with which they must comply, by implementing an Information Security Training and Awareness Program. The program will include both periodic training classes, and an ongoing security awareness campaign designed to maintain vigilance. New employees will receive information security training as part of the orientation process. All employees will receive mandatory training on at least an annual basis. Once trained, employees will sign an agreement that they understand and will comply with OPIC's information security policies. Information Owners and Information Custodians will also provide training to information users regarding the security policies and procedures for their specific systems.

6.3. Risk Management will be integrated into OPIC's IT decision-making and systems development lifecycle. OPIC's Risk Management framework will include:

6.3.1. Resource Classification – In order to ensure that appropriate levels of protection are applied to information resources, Information Owners will classify resources based on their sensitivity and their criticality to the agency. The ISSO will provide a framework that includes standards for assessing the criticality and sensitivity of systems, and determining minimum security requirements based on those assessments. Information Owners will use this framework to classify their resources.

6.3.2. Risk Assessment – The ISSO and information owners will implement processes to determine what risks to OPIC information resources exist, the likelihood of risk events occurring, and the impact on the organization if those events were to occur. Risk analysis will be used to make intelligent decisions regarding the use and protection of information resources.

6.3.3. Vulnerability Testing – In order to identify areas of risk so that they may be appropriately analyzed and mitigated, the ISSO and designated Information Custodians will perform periodic vulnerability testing on OPIC's systems.

6.3.4. Certification and Accreditation – To ensure that systems have adequate security commensurate with the level of risk, the ISSO will implement a formalized process to assess the risks and security requirements of each system, and determine whether the system's security is sufficient. Information Owners must ensure that their major information systems are certified and accredited.

6.4. A System Security Plan (SSP) will be required for each major information system. The SSP specifies the security requirements applicable to the system, and the protection mechanisms implemented to meet those requirements. The level of protection implemented will be commensurate with the level of risk, and the classification of the resources to be protected.

6.5. IRM will develop a *Continuity of Support Plan* and a *Disaster Recovery Plan* for providing access to critical information resources in the event of a disruption (*e.g.*, disaster, power outage, or other emergency). These plans will integrate with OPIC's Continuity of Operations Plan (COOP) which will be developed by OCFO with the participation from all OPIC departments. These plans will be updated and tested periodically.

6.6. Information Users must report suspected security incidents promptly to the ISSO or other appropriate official using OPIC's Incident Reporting procedures. The ISSO will implement an Incident Management process to handle incidents, including procedures for reporting, investigating, resolving, and documenting

incidents, as well as procedures for coordinating with, and reporting incidents to, FedCIRC and other appropriate parties.

6.7. Failure to comply with this directive may result in loss of use, or limitations on use, of OPIC information resources; disciplinary or adverse actions; or legal action, including termination or referral for criminal prosecution, as appropriate.

7. AUTHORITY:

7.1. Homeland Security Presidential Directive /HSPD-7, December 2003.

7.2. Federal Information Security Management Act (FISMA), PL 107-347, December 2002.

7.3. OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 2000.

7.4. OMB Memo M-99-20, Security of Federal Automated Information Resources, June 1999.

7.5. The Privacy Act, as amended, PL 93-579, January 1999.

7.6. Presidential Decision Directive 67, Continuity of Operations, October 1998.

7.7. Clinger-Cohen Act of 1996, PL 104-106, February 1996.

7.8. Computer Abuse Amendments Act of 1994, PL 103-322, September 1994.

7.9. Computer Security Act of 1987, PL 100-235, January 1988.

7.10. Computer Fraud and Abuse Act of 1986, PL 99-474, October 1986.

7.11. Foreign Corrupt Practices Act of 1977, as amended, PL 95-213, December 1977.

8. EFFECT ON OTHER INTERNAL RULES

8.1. Supersedes Directive 00-01, Information Systems Security Program, dated 03/01/01.

8.2. Rescinds Directive 98-02, *Use of the Internet and Electronic Mail*, dated 1/19/01.

By Order of the P&CEO

_____ October 20, 2004

Peter S. Watson **Date**
President and Chief Executive Officer

Office of Primary Responsibility: Office of the Chief Financial Officer, IRM.