Overseas Private Investment Corporation

OCFO/IRM

Information Systems Security Program (ISSP) Handbook

October 2004

This Handbook constitutes OPIC's Information Security Program procedures and guidelines, and incorporates OPIC policy for protecting unclassified information resources. All OPIC employees and contractors are responsible for complying with the policies and procedures contained herein, as well as with OPIC’s Information Systems Security Program Directive.

The OPIC Information Systems Security Officer (ISSO) is responsible for updating and maintaining this Handbook.

Security questions may be directed to:

Juliette Sheppard
Information Systems Security Officer
Information Resources Management
Office of the Chief Financial Officer
(202) 336-8541

TABLE OF CONTENTS

SECTION 1:

INTRODUCTION

1.1 What Is Information Security?

"Information security" refers to protecting information resources from being misused, either intentionally or accidentally. This includes protecting these resources from being lost, stolen, destroyed, or altered in an unapproved manner, as well as using these resources for illegal, unethical, or other inappropriate purposes.

Information resources include equipment and software that are used to process information, as well as the information itself. Computer equipment, telephones, fax machines, network connectivity (including Internet connections and dial-up accounts), software programs, databases, documents (both electronic and printed), and even personnel, are examples of information resources.

1.1.1 Why Is Information Security Important to OPIC?

OPIC has many critical and sensitive information resources to protect, including computer equipment, software, business data, client information, intellectual property, and confidential personnel records. The safeguarding of all of these information resources is vital to the continued operation and success of OPIC.

As a federal entity, OPIC faces a variety threats, ranging from terrorist acts to theft to accidental exposure/alteration of data. Inherent vulnerabilities also exist in the computer systems themselves. Each of these threats and vulnerabilities, when targeted at critical assets, can have a serious impact on the ability of OPIC to perform its mission.

1.1.2 Why Should Information Security Be Important To You?

By helping to safeguard OPIC information resources, you are helping to secure the tools needed to perform your duties, as well as protecting the continuation of OPIC's mission. Additionally, there are federal and local laws and regulations that specify information security responsibilities and rules for everyone who uses information resources at OPIC. Under these laws, you could be held personally accountable, and fined, or even jailed, for security violations or lack of due diligence.

1.2 What Is the Information Systems Security Program?

The OPIC Information Systems Security Program (ISSP) is a comprehensive set of initiatives designed to protect critical OPIC information resources so that they can be used to support OPIC's mission. The ISSP is also intended to ensure that OPIC is compliant with all federal regulations and other applicable laws, and to protect OPIC's reputation.

The program includes policies and procedures that specify how to securely and legally use information resources at OPIC. Also included is a comprehensive set of activities to promote security awareness and educate everyone at OPIC on their information security responsibilities.

1.2.1 What Is Included In The Program And How Is The Program Structured?

OPIC Management Directive 05-01 provides a charter for the Information Systems Security Program, and is based on legal requirements, federal government standards, and OPIC management objectives.

A set of OPIC Information Systems Security Policies (ISSPs) then specifies the "rules" for using and protecting information resources. Each policy discusses a specific security topic or type of information resource. The policies incorporate requirements and guidelines, roles and responsibilities, penalties for violations, the reason for each policy, and other important information pertaining to the particular security topic.

Standards and procedures provide step-by-step details on how to meet the requirements specified in the policies. Essentially, these documents provide the details for meeting the requirements of the policies.

To make it easier for you to understand the information security requirements, and your security responsibilities, we have developed this Handbook. The Handbook serves as your primary reference for understanding and meeting your information security responsibilities.

Additionally, information security training is provided, and required, for all OPIC personnel, to make sure that everyone understands OPIC security policies and maintains awareness of security issues. (More information on the information security training program is provided later in this Handbook)

1.3 What Happens If OPIC Information Security Policies Are Violated?

If employees are found to be knowingly, willfully, or negligently in violation of any OPIC information security policy or any of the provisions in this Handbook, they will be subject to administrative or disciplinary actions, civil remedies and criminal penalties, including, but not limited to:

- Loss or limitations on use of information resources,
- Disciplinary action, from warning to termination of employment, and/or
- Referral for criminal prosecution.

1.3.1 What Is An Information Security Violation?

An information security violation is any breach of OPIC information security policies, procedures or guidelines, whether or not the confidentiality, integrity, or availability of information is actually compromised. Information security violations may occur knowingly, willfully, or through negligence. Any action or a failure to adhere to OPIC information security policies is considered a security violation.

Examples of information security violations include, but are not limited to:

- Failure to comply with OPIC information security policies and practices, including those outlined in this Handbook.
- Using OPIC information technology resources to violate Federal or state administrative, legislative, judicial or criminal laws or procedures.
- Assisting staff, contractors, or any external entities or individuals in performing any information security offense.

1.3.2 What Determines The Severity Of A Violation?

The significance of an information security violation does not depend only on whether the confidentiality, integrity, and availability of information are actually compromised; it depends on the intentions and attitudes of the individual who commits the violation. Access to OPIC information systems is a privilege that may be changed or revoked at the discretion of management. Ability and willingness to follow the rules for protection of OPIC information systems is a prerequisite for maintaining access to those systems.

1.3.3 How Does OPIC Handle A Violation?

Security violations come to OPIC's attention in several ways: the OPIC ISSO becomes personally aware of a violation (*e.g.*, during periodic system audits); an Information Owner reports a violation; or another employee reports a violation to the ISSO.

After receiving notification of a violation, the ISSO may initiate an inquiry into the incident to determine whether OPIC information security has been compromised. Based on the findings, the ISSO may refer the matter to the OPIC Security Officer for further action.

The specific circumstances of the violation determine what sanctions, remedies or penalties OPIC will pursue. Based on the nature of the suspected violation, OPIC will follow the procedures set forth in OPIC's Employee Relations Management Directive, 94-24.

1.3.4 Can An Action Taken As A Result Of A Violation Be Appealed?

Individuals wishing to appeal a warning letter, reprimand or other action related to an information security violation must follow the procedures outlined in OPIC's Employee Relations Management Directive, 94-24.

1.4 Who Is Responsible for Information Security?

EVERYONE who uses any information resource at OPIC shares in the responsibility to protect that resource and to use it appropriately. This includes employees, contractors, interns, temporary workers, and even visitors.

1.4.1 What Are The Information Security Roles At OPIC?

Your information security responsibilities are based on your assigned security role. For example, someone who administers a computer system will have different security duties than someone who uses the system to look up or enter information.

The information security roles at OPIC are:

- Information Users are individuals who use or have access to OPIC's information resources, including employees, interns, temporary workers, contractors, vendors, and visit ors. When you are using any kind of OPIC information resource, or have access to any OPIC, client, or government data, you are an Information User.
- 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. It is crucial that Supervisors serve as a good example for their employees to follow, as well as helping them to understand and meet their information security responsibilities.
- 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. For example, the initial owner may be the person who writes a document, creates a database, or purchases a piece of equipment. Once created or installed, the individual's respective OPIC business unit becomes the Owne r, with the Departmental Vice President of that unit taking official responsibility.
- Information Custodians are individuals who develop, implement, maintain, or administer information resources on behalf of Information Owners. For example, IRM staff (inclu ding system engineers, database administrators, application developers, etc.) often serve as custodians for systems or data owned by OPIC business units.

1.4.2 Are There Specific Individuals Who Have A Special Role In OPIC Security?

In addition to the general security roles, there are a few individual positions that have specific security responsibilities. These include:

- The Information Systems Security Officer (ISSO) is the individual designated within OPIC to develop and operate the information security program. The ISSO is responsible for ensuring that OPIC complies with federal information security requirements and other applicable laws, and that OPIC resources are adequately protected.
- The OPIC Security Officer is the individual responsible for the security of OPIC facilities, personnel, and classified information. The OPIC Security Officer's may also assist the ISSO with investigations of violations and is responsible for granting, denying, suspending, reducing or revoking security clearances.
- The Designated Approving Authority (DAA) is the person who certifies and accredits information systems for operation on the OPIC network. This role is filled by the CIO or other designated high level OPIC executive.

1.4.3 How Do You Know What Role You Are Assigned?

Individuals may serve in multiple roles, depending on the different aspects of their jobs. For example, a Departmental Vice President may serve as an Information Owner for a particular resource, as a Supervisor for some employees in his/her department, and as an Information User.

The above role descriptions should help you determine your security role(s). It is up to you to find out which roles apply to you, and to understand and perform the responsibilities associated with those roles. If you are unsure which role(s) apply to you, please consult your supervisor or the ISSO for further guidance.

1.4.4 What Are The Responsibilities Of Each Security Role?

The remainder of this Handbook is organized by security role. Each section focuses on the responsibilities of a specific role. You should read the sections for each of your roles and make sure that you fully understand the responsibilities discussed in those sections.

Information Users	➡	SECTION 2: Guide For Information Users
Supervisors	➡	SECTION 3: Guide For Supervisors
Information Owners	➡	SECTION 4: Guide For Information Owners
Information Custodians	➡	SECTION 5: Guide For Information Custodians

1.5 Where Do I Get More Information?

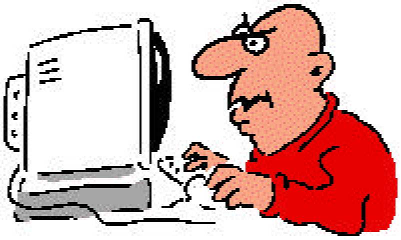
Copies of the OPIC Information Security Directive and the supporting policies, as well as an acronym list and a glossary, are provided in the Appendices of this Handbook. Additional information security information will be posted on the OPIC Intranet.

1.6 Who Can I Contact If I Have Questions?

If you have any questions about information security, please contact the OPIC Information Systems Security Officer (ISSO), Juliette Sheppard.

SECTION 2:

GUIDE FOR INFORMATION USERS



2.1 Understanding And Accepting Your Information Security Responsibilities

An important aspect of OPIC's Information Systems Security Program (ISSP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making Information Users aware of their security responsibilities and teaching them correct practices can OPIC reduce the level of security risk to its information systems.

Many components of OPIC's ISSP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into OPIC's program. Ensuring that you gain an understanding of your responsibilities is vital to OPIC because without your knowing the necessary security measures (and to how to use them), OPIC's information security will not be effective.

As someone who uses or has access to OPIC's information resources[1], you are referred to as an "Information User." Whether you are a regular employee, an intern, a temporary worker, or a contractor, information security is your personal responsibility, and you serve a critical role in protecting the resources you have been granted to use. As such, you are responsible for familiarizing yourself with, and abiding by, the policies and procedures outlined in this Handbook.

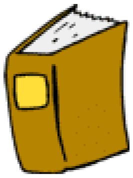
2.1.1 What Are The Responsibilities Of An Information User?

Your responsibilities are outlined throughout this section of the Handbook. However, here is a summary of some of your responsibilities:

- You must review, understand and accept your information security responsibilities.
- You must maintain awareness of information security policies by participating in OPIC's information security training program and by reviewing this Handbook.
- You should discuss with your supervisor or the ISSO any information security policies or procedures that you do not understand.
- You must protect OPIC information resources in your possession from theft, loss, damage and unauthorized activities including disclosure, modification, deletion, and misusage; and immediately report any loss, theft or damage to those resources.
- You must obtain, use, or disclose OPIC information only in an authorized fashion and only for authorized purposes.
- You must exercise due diligence to prevent accidental misentry, modification, or deletion of data.
- You must act responsibly so as to ensure the ethical use of OPIC information resources in compliance with the Standards of Ethical Conduct for Employees of the Executive Branch and OPIC's Ethics Program.
- You must promptly report any suspected violations of OPIC security policies to the ISSO, the Information Owner, or your supervisor.

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

2.1.2 Reviewing and Understanding OPIC Information Security Policies



This Handbook provides information and instructions for Information Users on:

- Fulfilling your security responsibilities (*e.g.*, completing annual information security training, completing a User Security Agreement, maintaining security awareness, and reporting security incidents);
- Auditing and privacy considerations;
- Acceptable and unacceptable use of OPIC information resources; and
- Policies and procedures you must follow when using OPIC information systems (such as remote access, password selection, etc.)

You should also take the opportunity to review the Information Systems Security Program (ISSP) Directive and detailed Information Systems Security Policies (ISSPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have questions, please ask your supervisor or the ISSO for clarification.

2.1.3 Completing OPIC's Information Security Training Program

For more information on Information Security Training, see OPIC ISSP-04, *Security Training and Awareness*.

The Federal Information Security Management Act (FISMA) requires every federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access and on a periodic refresher basis.

Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of OPIC information resources. Information security policies and standards cannot be effective unless everyone at OPIC, regardless of level in the organization, is aware of the importance of information security, understands OPIC information security procedures, and performs required practices.

For these reasons, all employees, including interns, as well as personal services contractors, industrial contractors, consultants, and experts hired on contract, must fulfill OPIC's information security training program. ISSP-04, *Security Training and Awareness*, outlines OPIC's training policy, which can be summarized as follows:

All OPIC Information Users will complete information security training. This training consists of the following three activities:

1. Information security training is incorporated into the new hire and new contractor orientation processes. Training must be completed within 30 days of employment or initiation of contract.
2. All Information Users must complete annual information security refresher training.
3. Information Custodians and other personnel with responsibilities related to administering and securing systems are provided with enhanced security training applicable to their functions.

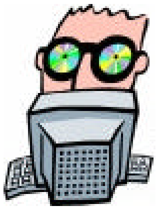
Information security training may be in the form of classroom, one-on-one, computer-based, or other format, as determined by the ISSO.

2.1.4 Completing The User Security Agreement

See ISSP-04, *Security Training and Awareness,* for a copy of the agreement

All OPIC employees, including individuals hired in the competitive or excepted civil service, as well as personal services contractors (PSCs), industrial contractors, consultants and experts hired on contract, must acknowledge and agree to comply with OPIC's information security policies and procedures in order to have access to OPIC information resources. The "Agreement To Comply With OPIC Information Security Policy" is to be signed annually by each employee upon completion of information security training.

2.1.5 Maintaining Security Awareness



One of OPIC's information security program goals is to help Information Users maintain security awareness on an ongoing basis. Information Secur ity is not a one-time event, but a continuous effort and "state of mind." This is achieved by reinforcing appropriate behaviors and mindset on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

OPIC's security awareness program sets the stage by changing organizational attitudes to realize the importance of security and the adverse consequences of its failure. It also reminds users of the procedures that must be followed. Hopefully, awareness will stimulate and motivate all OPIC staff to care about security and remind everyone of important security practices.

The ISSO will periodically issue information notices to OPIC employees to remind them of basic security practices (*e.g.*, protecting your passwords). The ISSO will also provide just-in-time brown bag discussions and briefings on special topics (*e.g.*, spam filtering).

It is your responsibility to exercise security awareness at all times when performing your OPIC duties, and to take an active part in protecting OPIC resources.

2.2 Reporting Information Security Incidents

You must immediately report any suspected information security incidents so that OPIC may respond in a timely manner to correctly handle the incident, minimize disruption of critical information services, and minimize loss or theft of sensitive and mission-critical information.

Your cooperation and participation in reporting security incidents is vital to OPIC's maintaining the security of its information resources. 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.

2.2.1 What Is An "Information Security Incident?"

An "information security incident" is any activity or event has occurred that threatens the availability, integrity, or confidentiality of information resources, or any action that is in violation of security policies.

Examples of information security 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 or contain OPIC data.
- Attempts by unauthorized individuals to gain access to OPIC information or systems.
- Accidental disclosure, modification, or destruction of information.

A "critical information security incident" is an incident that will result in a severe impact to OPIC resources if not addressed immediately.

2.2.2 How To Report An Information Security Incident

For more information on Reporting Security Incidents, see OPIC ISSP-05, *Incident Reporting*.

You must report suspected incidents to the ISSO, the Customer Service Center (CSC), the Information Owner, or your supervisor (in this order of preference) as quickly as possible. You must report critical security incidents immediately. You may report incidents either verbally or in writing. It is recommended that you retain proof that you reported the incident.

After you notify the ISSO, the Information Owner or your supervisor, you may be required to document relevant information about the suspected incident. You may also be requested to assist the ISSO or system administrators with resolution of the incident. Your full cooperation in resolving the incident is required.

2.3 Does OPIC Audit The Use Of Information Resources?

For more information on Auditing, see OPIC ISSP-13, *Audit Trails*.

OPIC regularly audits the use of information resources to ensure accountability for the use of those resources, detect security violations, and to proactively scan for vulnerabilities. All use of OPIC information resources may be monitored by OPIC at any time. You should not have an expectation of privacy or anonymity while using OPIC information resources, including email and Internet access.

As an OPIC Information User, you are governed by OPIC's authorized limited personal use policies. By using OPIC information systems and other office equipment, you imply your consent to disclosing the contents of any files or information maintained or passed-through those information systems or office equipment. As required by law, OPIC may disclose information generated on its information systems to law enforcement or oversight organizations. The information security program in no way removes any privilege or protection afforded OPIC employees under the Privacy Act, the Freedom of Information Act, or any other law or regulation.

In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated records of access to and alteration of information systems and data are maintained. To accomplish this, a record of activity (or "audit trail") of system and application processes and user activity of systems and applications is maintained. This is used to investigate security incidents, monitor use of OPIC resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. Audit trails also assist in detecting security violations, performance problems, and flaws in applications.

System administrators (on behalf of Information Owners) have the ability to audit network logs (via server, application, router, firewall and other major network device transaction logs), employ monitoring tools, and perform periodic checks for misuse. The ISSO is required to conduct periodic reviews of audit logs.

2.3.1 What Is An "Audit Trail?"

In the context of computer systems, an "audit trail" is a record of activities that occur on the system. The audit trail is generally composed of log files that track such things as user login, file access, system modification, resource usage, and other activities. These files can provide information regarding any actual or attempted security violations that may have occurred on the system, and may serve as evidence for disciplinary or criminal action.

2.3.2 Can I Expect Any Privacy When Using OPIC Information Resources?

No. You do not have a right, nor should you have an expectation, of privacy while using OPIC information systems. When you use OPIC information systems, it is with the understanding that such use is not private and is not anonymous.

There is no right of privacy on the part of any individual regarding any information transmitted, stored or received via OPIC's information systems. Use or access to the network constitutes consent to OPIC's limited personal use policy, and to the monitoring, storage, retrieval or disclosure of any information transmitted, stored or received via the network for any purpose, including employee discipline, contractual remedies or criminal prosecutions.

Avoid using OPIC information systems for any activities that you wish to keep private.

2.4 Acceptable Use of OPIC Resources

For more information on Acceptable Use, see OPIC ISSP-01, *Acceptable Use of Information Resources*, and OPIC Management Directive 94-04.

OPIC information resources are for use only by authorized persons and only for authorized purposes. Access to computers, systems, networks, and data owned by the government is a privilege that imposes certain responsibilities and obligations and that is subject to governing laws. OPIC's authorized limited personal use policy is intended to promote the efficient, ethical and lawful use of OPIC information resources, yet allow employees the opportunity for limited personal use of those resources.

As an OPIC Information User you must act in a legal, ethical, responsible, and secure manner while using OPIC information systems. Inappropriate use of information resources exposes OPIC to risks including compromise of systems and services, legal issues, financial loss, and damage to reputation.

You are also responsible for exercising good judgement in using OPIC information resources efficiently. You should use your common sense to do what a reasonable person would do to protect OPIC information resources.

The following two sub-sections discuss acceptable and unacceptable use of OPIC information resources.

2.4.1 What Is Acceptable?

You may use OPIC-provided information resources only for authorized purposes. Authorized purposes include official use, which is use for OPIC-related business in accordance with your job functions and responsibilities. Authorized purposes also include emergency use, such as sending an emergency email to notify a spouse of illness during working hours. As set forth in OPIC Management Directive 94-04, authorized purposes also include limited personal use of information resources if that use does not result in a loss of employee productivity, does not interfere with official duties or business, and involves "minimal additional expense" to the government.

Authorized limited personal use may incur only "minimal additional expense" to OPIC in areas including but not limited to:

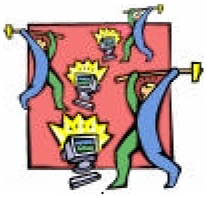
- Communications costs (*e.g.*, telephone charges, telecommunications traffic, etc.).
- Use of consumables in limited amounts (*e.g.*, paper, ink, toner, etc.).
- General wear and tear on equipment.
- Data storage on information technology devices (*e.g.*, moderate email message sizes and quantities).

Examples of authorized limited personal use include minimal or non-duty use of phones or computers to check Thrift Savings Plan or other personal investments, seeking employment, dealing with Employee Assistance issues, communicating with volunteer charity organizations, and performing academic work/training that does not interfere with completing your job responsibilities.

All use must be in compliance with OPIC information security policies.

2.4.2 What Is Not Acceptable?

OPIC information resources may be used only for authorized purposes, which are discussed in the preceding sub-section. In addition to understanding OPIC's authorized use policy, you should be aware of the following specific activities, which are *strictly prohibited* while using OPIC information resources:



- You may not use OPIC information personal property systems to maintain or support a personal private business, including use personal property of those systems to assist relatives, friends, or other persons in such activities. This prohibition includes personal activities that are for commercial purposes, that support "for-profit" activities or are intended to generate income (*e.g.*, electronic day-trading), or that support other outside employment or business activity (*e.g.*, consulting for pay, sales or administration of business transactions, sale of goods or services, or acting as a real estate agent).
- You may not engage in any outside fund-raising activity, endorse any product or service, participate in any lobbying activity, or engage in any prohibited partisan political activity using OPIC resources.
- You may not access or disseminate material that is offensive or harassing in nature, including material that disparages others based on race, religion, ethnicity, gender, sexual orientation, age, disability or political affiliation. You may not access or disseminate sexually explicit or sexually oriented messages, images, or sounds.
- You may not acquire, use, reproduce, transmit, or distribute any controlled information including computer software and data, privacy information, copyrighted or trademarked material or material with other intellectual property rights (beyond fair use), or proprietary data, without authorization.
- You may not disseminate trade secrets or business sensitive information, except as permitted by law or regulation, including posting agency info to external newsgroups, bulletin boards or other public forums without authority.
- You may not transmit, store, or process classified data except as authorized and in accordance with OPIC Directive 94-14, *OPIC Security Program*.
- You may not conduct any personal activity that could create the perception that the communication was made in your official capacity as a Federal Government employee, unless appropriate OPIC approval has been obtained.
- You may not create, access or download material related to illegal activities (*e.g.*, gambling, illegal file swapping, software piracy, etc).
- You may not perform any action that would otherwise violate the Standards of Ethical Conduct for Employees of the Executive Branch.
- You may not conduct any personal use that could generate more than minimal additional expenses to OPIC and/or cause congestion, delay, or disruption of service to any OPIC system or equipment (*e.g.*, downloading large video or sound files). This prohibition includes executing a program that may hamper normal OPIC computing activities.
- You may not send unsolicited email messages (spam) or create, copy, transmit, or retransmit chain letters or other unauthorized mass mailings, regardless of the

subject matter.

- You may not use OPIC's systems as a platform to gain unauthorized access to data or other systems.
- You may not access information resources, data, equipment, or facilities in violation of any restriction on use. Further, you may not access OPIC systems that are not necessary for the performance of your duties. Nor may you perform functions that are not related to your job responsibilities on authorized systems.
- You may not make unauthorized changes to OPIC computer resources, including installation of unapproved software or interference with security measures (*e.g.*, audit trail logs and antivirus software).
- You may not add components or devices (*e.g.*, PDAs, thumb drives, cameras, etc.) to OPIC desktops without explicit approval from the Director of Technical Services.
- You may not connect unauthorized devices (including contractor or personal laptops) to the OPIC computer network without approval from the Director of Technical Services.
- You may not copy proprietary software (or software licenses) or OPIC business data for personal or other non-United States government use.
- You may not perform unauthorized security scanning, network monitoring, or data interception that is not part of your regular job duties.
- You may not use another person's computer account, with or without his or her permission.
- You may not reveal system passwords (*e.g.*, network login password, FPPS password, database password, etc.) to anyone who is not specifically authorized to use them. This includes revealing account passwords to others, including family and other household members, when government work is being done at home.
- You may not knowingly, without authorization, introduce a program into the OPIC environment that could hamper normal computer operations (*e.g.*, virus, spyware).
- You may not intentionally corrupt or damage any information resource.
- You may not remove any OPIC information resource from the OPIC premises without authorization.
- You may not deny, or interfere with, the legitimate use of resources by other OPIC personnel.
- You may not otherwise violate any existing information security law, rule, regulation, OPIC policy or OPIC implementing procedure.

2.5 Access To OPIC Information Resources

For more information on Access Controls, see OPIC ISSP-11, *Access Controls*.

You may only access resources to which you have been authorized, and you may not circumvent the permissions granted to your accounts in order to gain access to unauthorized information resources.

You may access OPIC information systems only during standard OPIC business hours, unless otherwise permitted by IRM for legitimate business purposes. You will not be permitted access to the OPIC network (OPICNET) during nightly scheduled backup periods unless approved by the Director of Technical Services.

2.6 Screening and Authorization

For more information, see OPIC ISSP-16, *Personnel Security*.

Access to OPIC information resources is limited to those persons who have been appropriately screened and authorized. Any access granted to you to OPIC information resources will be based on the requirements of your duties, and you must have appropriate clearance for the sensitivity level of the resources to which you are granted access.

Therefore, you will be subject to at least a minimal background check (if you have not had a previous investigation and/or do not have any recent, documented positive suitability determination) prior to being granted access to sensitive information.

Additionally, if you are a contractor or other non-OPIC employee, you must sign a non-disclosure agreement protecting any sensitive data to which you will have access.

2.7 Passwords & UserIDs

For more information on Passwords and UserIDs, see OPIC ISSP-32, *Password Management*.

OPIC reduces the risk of excessive or unauthorized disclosure of its information resources through the application of userIDs and passwords. For example, your access to OPIC information resources is limited to the access required for you to perform your duties. You have been granted specific access privileges on each system, and those access privileges are associated with your userID (*i.e.*, logon name). Your password serves as authentication of your identity, and is used to grant or deny access to OPIC information systems. If you choose a poor password, it can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

As an Information User, *you may be responsible for any activity initiated by your userID* since you are the only person who should have your logon information. You must protect your user account(s), and not allow anyone else to use your account or use your computer while logged in under your account (except as required for system administration). In order to protect your user credentials, you must adhere to the following rules:

- Do not lend or divulge your password to other persons, including individuals purporting to be system administrators.
- Change your password immediately upon your initial user logon, at least every 90 days, and any time it is suspected that your password may have been compromised.
- Never make your password visible on a screen, in written form (*e.g.*, on sticky notes), or on any other output device unless it is secured in an approved, locked area.

- When you leave your computer unattended, you must either log out or invoke protection of your system (*e.g.*, a password-protected screensaver).
- Never send your password via email.
- Avoid using the "remember password" feature on web sites and other applications.
- Choose effective passwords (see the following sub-section).

2.7.1 What are the guidelines for choosing an effective password?

Adhere to the following guidelines for selecting effective passwords:

- Your password should be at least 8 characters and contain a combination of letters, numbers, and special characters.
- You may not use the same password at OPIC that you use for any non-OPIC computer accounts (*e.g.* an account on an Internet website).
- Your password cannot be reused for at least four changes. It is best not to reuse any previous password at all.
- You may never assign a login account a password that is the same string as your userID or that contains your userID (*e.g.*, "bob123" is not an appropriate password for user "bob").
- You may never set any password equal to the null string (*i.e.*, a blank password). This is equivalent to no password at all.
- Your password should not be a dictionary word in any language.
- Your password should not contain any proper noun or the name of any person, pet, child, or fictional character.
- Your password should not contain any employee serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.
- Your password should not contain any simple pattern of letters or numbers, such as "xyz123."
- Your password should not share more than 3 sequential characters in common with a previous password (*i.e.*, do not simply increment the number on the same password, such as fido1, fido2, etc.).
- You should use a password that is easy to remember (*e.g.*, a phrase, line from a song, or nonsense words) and that you can type quickly.

If you need assistance with selecting an appropriate password, please contact the Customer Support Center (CSC).

2.8 Physical Access

For more information on Physical and Environmental Security, see OPIC ISSP-17, *Physical and Environmental Security*.

OPIC information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas must be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

As an Information User, your physical security responsibilities include:

- Admittance to areas containing sensitive information resources will be limited to OPIC employees and other individuals (*e.g.*, contractors) who have been specifically authorized access to them. If you are assigned to an area containing sensitive information resources, you must escort all personnel without an appropriate security clearance through that space. If you are unsure of an individual's level of clearance, check with either your Departmental Security Officer or your department's Administrative Assistant (AA). These individuals have access to information on the current level of security clearance of every OPIC employee and contractor.
- When uncleared personnel are present in these areas, you must protect sensitive information from observation, disclosure, or removal. This includes storing away documents and positioning all computer monitors to prevent viewing by unauthorized persons.
- You should challenge any unrecognizable and unescorted person in OPIC's space to show appropriate identification. Notify security immediately so that they may escort the person out of OPIC's space.

Of course, you must immediately report to the OPIC Security Officer any incident or condition contrary to OPIC's physical or environmental security.

2.9 Remote Access

For more information on Remote Access, see OPIC ISSP-25, *Remote Access*.

You use remote access capability any time you access OPIC's network while outside the office (*e.g.*, while traveling on business or while telecommuting). Remote access to OPIC via dial-up or other connectivity poses an increased risk of intrusion into OPIC information systems by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of the OPIC network also lacks the protections afforded by OPIC's corporate firewall and other protections. For these reasons, remote access is governed by special security measures to mitigate the increased security risks that are present in this situation.

IRM has put in place technical measures to ensure that remote access is provided in a secure manner. For example, telecommuters must use multiple methods of authentication to access the OPIC network from their OPIC laptops (*i.e.*, they must use their network passwords in conjunction with tokens). Additionally, information transferred over remote access connections is encrypted to protect it from unauthorized disclosure.

As an Information User you have certain responsibilities when using remote access:

- You must observe all of the same security policies when accessing OPIC information resources remotely that you would at the office.

- Any personal equipment, including personal home computers, used to connect to OPIC's information resources must meet OPIC remote access security requirements, including having an approved antivirus program installed and being configured with the latest software updates.
- You may not store sensitive OPIC data on non-OPIC computers.
- You must protect your remote access credentials, devices and connections from disclosure to, or use by, unauthorized persons, including family members.
- You may not change the hardware, software, or security configuration of OPIC remote access computers.
- To prevent unauthorized users from accessing sensitive OPIC information via open ports, remote access sessions and open terminal windows must never be unattended. You must log out rather than terminate a remote session when finished. You must also wait until you receive a confirmation of your log-out command from the remotely connected OPIC machine before you leave the computer you are using.
- You must immediately report any suspected unauthorized use of your remote access account or any damage to or loss of OPIC computer hardware, software, or data that has been entrusted to your care.

If you have any questions regarding the requirements above, you should contact the ISSO or the Customer Support Center.

2.10 Mobile Computing

For more information on Mobile Computing, see OPIC ISSP-22, *Mobile Computing*.

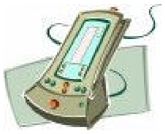
"Mobile devices" are any portable devices that can store or process data. Examples include laptop computers and PDAs (*e.g.*, Blackberry, Palm).

The use of these devices outside the OPIC office environment poses risks to the devices and the information they contain. Mobile devices may also present a hazard to other OPIC resources upon their return to the OPIC office (*e.g.*, by spreading a virus that was obtained outside the office). These devices also have the capability for direct connectivity to the Internet or other networks outside of the OPIC network which lack the protections afforded by OPIC's corporate firewall and other protections. That is why you must take additional security measures to reduce the risks presented by mobile computing.

OPIC has put in place technical measures to ensure that mobile devices are assigned to you already have some security in place. For example, all laptops have antivirus software installed. However, you have a major role in protecting the security of these devices.

Your responsibilities as a mobile computing Information User who uses include:

- To ensure that devices are inventoried and tracked, you will be asked to sign out laptops and other mobile computing devices before they are given to you.
- You must back up any data that is stored on the mobile device on a regular basis.
- You must take all reasonable precautions to protect mobile devices from loss, theft, tampering, and damage.



- You must ensure that the device is not used by unauthorized persons or for unauthorized purposes.
- You must immediately report to the Customer Service Center the loss, theft, tampering, unauthorized access, or damage of any OPIC mobile device.

2.11 Wireless Networking

For more information on Wireless Security, see OPIC ISSP-27, *Wireless Security*.

You may find that wireless communications and devices are convenient, flexible, and easy to use. Wireless devices transmit data without the use of cables. Examples of wireless communications include radio transmissions, cell phones, PDAs, laptops with wireless network cards, and other devices such as wireless headphones. Infrared devices such as cordless computer keyboards, and cordless mouse devic es are also included.

In addition to the risks that apply to all networks, wireless connectivity has additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be easily intercepted by anyone nearby who is actively listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this open architecture to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Additionally, like any mobile devices, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to OPIC networks via the hijacked or stolen device.

Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted over it.

As an Information User, you are required to:

- Obtain approval from the Customer Service Center before using or deploying any wireless technology to access or transmit OPIC information. This rule applies regardless of whether these devices are owned by OPIC.
- Safeguard wireless devices in your possession and safeguard OPIC information resources being accessed or transmitted via any wireless technology.
- Be aware that wireless interface cards are explicitly prohibited from being used at OPIC facilities.
- Immediately report to the Customer Service Center the loss, theft, tampering, unauthorized access, or damage of any OPIC wireless or handheld device.

2.12 Access to the Internet

Employees will access the Internet only through OPIC-approved Internet access points (e.g. OPIC firewalls). Any form of communication to or from workstations outside the internal (trusted) network that bypasses these protected access points is strictly prohibited without authorization. This includes the use of modems, leased lines to other networks, or wireless connectivity. Access to the Internet from outside of OPICNET (e.g., using laptop while traveling) is not governed by this policy. However, such access must be compliant with OPIC Remote Access and Mobile Computing policies.

2.13 Electronic Mail

For more information on Electronic Mail, see OPIC ISSP-29, *Electronic Mail*.

Email is an essential tool used by OPIC to conduct its business. However, email is inherently insecure and presents many risks to information security. Email can be read, altered, or deleted by unknown parties without the permission of the sender or recipient. Email can also be used to distribute viruses and other harmful programs that pose a threat to OPIC resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

As an Information User, you have certain responsibilities in supporting email security:

- You must understand that email can be intercepted or altered without your knowledge (both within and outside of OPIC.)
- You may only send OPIC data via OPIC owned or operated email systems.
- You are not permitted to forward OPIC email or attachments to personal accounts managed by public email or internet service providers where the information might be compromised (e.g., hotmail, yahoo, etc).
- You are prohibited from using any OPIC email systems (or any other email systems accessed from OPIC computers) for prohibited purposes, as outlined in OPIC's *Acceptable Use of Information Resources* policy (ISSP-01) and Management Directive 94-04.
- You should not open attachments or click on links in messages from senders you do not know.
- You should report suspicious email messages to the Customer Support Center.
- To minimize spam and avoid waste of OPIC resources, you must avoid using your OPIC email addresses for personal correspondence on the Internet, especially if this includes giving out your official email address to Internet shopping sites, bulletin boards, and mailing lists (that are not related to your duties.)
- You should have no expectation of privacy while using OPIC's email system.
- You may not direct unauthorized messages to the All OPIC distribution group or other large groups of users.
- You must delete emails once they are no longer needed, in accordance with OPIC Record Management policies. On a periodic basis you must archive from the email server old emails that must be retained. Contact the Customer Support Center for information and instructions on how to do this.

2.14 Protecting Against Computer Viruses

For more information on Anti-Virus Measures, see OPIC ISSP-14, *Anti-Virus*.

Computer viruses may destroy data, make OPIC computers unusable, use OPIC's computers to attack other computers, or perform a variety of other malicious activities. To minimize risks associated with viruses, OPIC has implemented standard software and procedures to safeguard OPIC's servers, workstations, and remote access computers. The use of antivirus software is essential for protecting OPIC resources from the danger posed by computer viruses and other malicious programs. These programs check for viruses on OPIC's computers and attempt to remove them before they can spread or perform further damage.

Antivirus programs, however, take time to learn about each new virus that is created, during which the virus can do serious damage. Therefore, it is important that you become aware of the risks posed by viruses, and take steps to minimize OPIC's exposure to them.

As an Information User, you have the following responsibilities regarding virus protection:

- You may not unload or disable antivirus software for any reason.
- Any computer used for remote access to the OPIC network (*e.g.*, a laptop used for telecommuting or a home computer used to do OPIC work) must have approved antivirus software loaded and updated on a regular basis. You should contact the Customer Support Center for guidance on what antivirus software OPIC has approved for this purpose.
- You must notify the Customer Support Center immediately if your computer becomes infected with a virus.
- You must take steps to avoid introducing viruses into OPIC's computing environment, including:
  - Never open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and empty your email Trash folder.
  - Delete spam, chain, and other junk email without forwarding.
  - Never download files from unknown or suspicious sources.
  - *Never install any software on OPIC computers without specific permission from IRM.*
  - You must scan all portable media (*e.g.* floppy diskettes, CDs) for viruses before using them on an OPIC computer. This should be performed automatically by the antivirus software on your computer. However, it is a good idea to perform an extra manual scan of these media if they have been used outside of the OPIC environment (*e.g.*, if you brought a diskette in from home.) Contact the Customer Support Center for instructions on how to perform a virus scan.
  - If prompted to install downloaded applications, always Cancel

2.15 Telephone Security

For more information on Telephony Security, see OPIC ISSP-26, *Telephone Security*.

For further information on OPIC's policy on phone use, please consult the OPIC *Telecommunications Handbook*

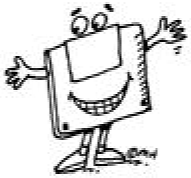
OPIC telephony resources include telephones, fax machines, and modems. These are vulnerable to a variety of security threats and are subject to the same security requirements and protections as other information resources.

As an Information User, you must adhere to the following rules when using the OPIC phone system or OPIC-issued cellular phones, in order to protect the information communicated:

- You should have no expectation of privacy when using the OPIC phone system or OPIC-issued cellular phones.
- You should understand that OPIC may audit use of these resources, as set forth in the OPIC Telecommunications Handbook, and that it is possible for third parties to tap or redirect phone calls outside of OPIC.
- You should never discuss sensitive information over a cell phone because of the ease of intercepting such communications.
- You may never discuss classified information over any phone that has not specifically been approved for such use. Contact the OPIC Security Officer if you require use of a secure phone line.
- You should make sure that the person on the other end of the conversation is who they say they are. You must not give out sensitive information (including agency credit card information) unless you are sure of the identity of the person who is on the other end of the line.
- You must be cautious when discussing sensitive information that the conversation cannot be overheard by unauthorized persons (*e.g.*, visitors to OPIC). You should minimize use of the speakerphone.
- You must obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.
- You must follow OPIC's Acceptable Use policy in using phone resources, just as you would with email or other information resources.
- You may not install modems or other telephony equipment without the explicit approval of the appropriate official (*e.g.*, the Director of Technical Services for modems and related telephony equipment).

2.16 Protecting Media

For more information on Backups and Media Management, see OPIC ISSP-19, *Backup and Recovery*, and OPIC ISSP-31, *Media Management*.



Information users often find the need to store data on "media" other than their OPIC computer hard drive. For example, floppy disks, zip drives, CDs, CD-ROMs, DVDs, flash drives, and backup tapes, are all commonly used types of "storage media". All of these must be handled, stored, and disposed of properly in order to protect the sensitive or critical OPIC data placed on them from unauthorized disclosure, damage, fraud, and abuse.

As an information user, you are responsible for adhering to the following when using storage media:

- You may store OPIC data only on approved media. Contact the Customer Service Center for assistance in identifying the appropriate storage media for your data.
- All storage media brought onto OPIC's premises or used with OPIC information systems must be scanned for viruses prior to use.
- You must take all reasonable steps to protect OPIC storage media in your possession from tampering or accidental damage.
- You are responsible for making your own backups of any data that is stored on media in your physical possession rather than on an OPIC server. Be aware that many threats exist that could cause the loss, corruption, or unavailability of data that is backed up on storage media. It is therefore essential that you maintain backup copies of all critical data that are stored on media so that they can be used to provide the continued availability and viability of these resources if unforeseen events occur. For example, you may copy your data to OPIC's network servers which are backed up daily.
- Special procedures must be applied to the handling and disposal of storage media that are used to store sensitive information, as described in the following two subsections.

2.16.1 What is the proper way to handle media that contains sensitive data?

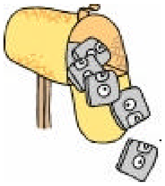
The following procedures must be followed when storing sensitive data on portable media:

- You must mark any media containing sensitive data with labeling that includes any special handling instructions.
- You must secure any media containing sensitive data when it is not in use or unattended. You should put it in a locked drawer, cabinet, or safe.
- If you send any media containing sensitive information through the mail or via a courier/messenger service, you must double-seal the media, with the outer envelope appropriately marked to reflect the level of sensitivity and the intended recipient.
- The delivery and receipt of media containing sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.
- You may never store national security classified information (*i.e.*, Top Secret,

Secret or Confidential information) on portable media unless you are authorized to do so and take security precautions required by law. Refer to the OPIC Security Handbook for information on storing classified materials.

- You must immediately report to the CSC, ISSO, or DTS the loss, theft, tampering, unauthorized access, or damage of any storage media that contain critical or sensitive OPIC data.
- When disposing of, or reusing, any media containing sensitive data, OPIC sanitization procedures must be followed (see next subsection).

2.16.2 What is the proper way to dispose of storage media?



Simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly. Therefore, it is important to properly "sanitize" any media that may contain sensitive information once the media and/or the data is no longer needed.

"Sanitization" refers to the process that is used to wipe data from storage media so that data recovery is impossible. The most common types of sanitization are destruction (*e.g.*, burning or smashing), degaussing (*i.e.*, demagnetizing), and overwriting.

OPIC has special software and a standardized process for sanitizing media. If you have media that should be sanitized, please contact the Customer Service Center for guidance and assistance with this process.

SECTION 3:

GUIDE FOR SUPERVISORS

3.1 Understanding And Accepting Your Security Responsibilities

An important aspect of OPIC's Information Systems Security Program (ISSP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can OPIC reduce the level of security risk to its information systems.

Many components of OPIC's ISSP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into OPIC's program. Ensuring that you gain an understanding of your responsibilities is vital to OPIC because without your knowing the necessary security measures (and to how to use them), OPIC's information security will not be effective.

As someone who supervisors OPIC information users, including regular employees, contractors, interns, and temporary workers, you are referred to as a "Supervisor." As such, you have specific security responsibilities. You are responsible for familiarizing yourself with and performing those responsibilities, as outlined in this Handbook.

3.1.1 What Security Responsibilities Does A Supervisor Have?

The primary information security responsibilities of a "Supervisor" fall into three areas:

- Ensuring that your employees are aware of, and trained on, their infosec duties.
- Assisting the ISSO and Human Resources with ensuring that your employees comply with OPIC information security policies and procedures.
- Reviewing information security reports from the ISSO regarding activities of your staff and taking appropriate action.

The specific duties will be outlined later in this section.

3.1.2 Reviewing and Understanding OPIC Information Security Policies

This section of the Handbook provides information and instructions for Supervisors on fulfilling your security responsibilities

You should also take the opportunity to review the ISSP Directive and detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have questions, please ask the ISSO to provide clarification.

3.2 Maintaining Security Awareness

One of OPIC's information security program goals is to help everyone at OPIC maintain security awareness on an ongoing basis. Information Security is not a one-time event, but a continuous effort and "state of mind." This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

As a Supervisor, it is your responsibility to help maintain your employees' information security awareness, and to take an active part in protecting the OPIC information resources that they use. You should also serve as a good role model for your employees regarding information security awareness.

3.3 Reporting Security Incidents

For more information on Reporting Security Incidents, see OPIC ISSP-05, *Incident Reporting*.

You must immediately report any suspected information security incidents so that the OPIC incident response team may respond in a timely manner to correctly handle the incident, minimize disruption of critical information services, and minimize loss or theft of sensitive and mission-critical information.

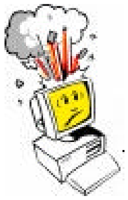
Your cooperation and participation in reporting security incidents is vital to OPIC's maintaining the security of its information resources. It is important that all supervisors maintain vigilance regarding information security, and immediately report any suspected incidents in order to minimize potential damage to OPIC.

Additionally, as a supervisor, you may receive reports of incidents directly from your employees. You need to communicate and escalate these incident reports to the ISSO or Director of Technical Services.

3.3.1 What Is A "Security Incident?"

A "security incident" is 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.

Examples of security 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 individuals to gain access to OPIC information or systems.
- Accidental disclosure, modification, or destruction of information.

A "critical security incident" is an incident that will result in a severe impact to OPIC resources if not addressed immediately.

3.3.2 How To Report A Security Incident

You must report suspected incidents to the ISSO, the Customer Service Center (CSC), or the Information Owner (in this order of preference) as quickly as possible. You must report critical security incidents immediately. You may report incidents either verbally or in writing. It is recommended that you retain proof that you reported the incident.

After you notify the ISSO, the CSC, or the Information Owner, you may be required to document relevant information about the suspected incident. You may also be requested to assist the ISSO, system administrators, or Human Resources with resolution of the incident. Your full cooperation in resolving the incident is required.

3.3.3 Incident Response

As a Supervisor, you may have to play a role in the incident response process. This could include such activities as:

- Confirming incidents reported by your staff.
- Assisting your staff with providing information to the ISSO for incidents that they have reported to you.
- Assisting the ISSO or designated personnel with investigating incidents involving your staff.
- Working with Human Resources on determining and implementing corrective actions for your employees who have committed security violations.

3.4 Employee Security Training Program

The Federal Information Security Management Act (FISMA) requires every Federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access and on a periodic refresher basis.

Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of OPIC information resources. Information security policies and standards cannot be effective unless everyone at OPIC, regardless of level in the organization, is aware of the importance of security, understands OPIC security procedures, and performs required practices.

For more information on Information Security Training, see OPIC ISSP-04, *Security Training and Awareness*.

For these reasons, all employees, including individuals hired in the competitive or excepted civil service (*e.g.*, student interns), as well as personal services contractors, industrial contractors, consultants, and experts hired on contract, must fulfill OPIC's information security training program. ISSP Policy #04, *Security Training and Awareness*, outlines OPIC's training policy.

As a supervisor, you are responsible for:

- Providing the opportunity for your employees to attend security training and review security policies and awareness materials.
- Taking an active role in ensuring that employees complete security training and awareness activities.
- Disciplining employees that do not comply with infosec training requirements.
- Helping your employees to understand OPIC information security policies.
- Ensuring that your employees understand their responsibilities.
- Communicating changes in policies and/or procedures to your employees.

SECTION 4:

GUIDE FOR INFORMATION OWNERS

4.1 Understanding And Accepting Your Security Responsibilities

An important aspect of OPIC's Information Systems Security Program (ISSP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can OPIC reduce the level of security risk to its information systems.

Many components of OPIC's ISSP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into OPIC's program. Ensuring that you gain an understanding of your responsibilities is vital to OPIC because without your knowing the necessary security measures (and to how to use them), OPIC's information security will not be effective.

As someone who has official responsibility for an OPIC information resource(s), you are referred to as an "Information Owner." As such, you have specific information security responsibilities. You are responsible for familiarizing yourself with and performing those responsibilities, as outlined in this Handbook.

4.1.1 What Security Responsibilities Does An Information Owner Have?

As an information owner, you are ultimately responsible for the information resources for which you have been assigned ownership. You must exercise due diligence to protect the confidentiality, integrity, and availability of those resources. In support of this duty, you have the following general responsibilities (which are detailed in this section of the Handbook):

- You must ensure that your resources are adequately protected, commensurate with their sensitivity and criticality, and the level of risk. This includes the planning and implementation of technical, managerial and operational security controls.
- You must ensure that your resources are in compliance with all OPIC information security policies, procedures and standards, as well as federal laws.
- You may delegate administration and maintenance of the resource to an Information Custodian, but must understand that you are still ultimately responsible for that resource, and thus need to actively monitor that custodianship.
- You must create and maintain thorough documentation of your resource and the security measures employed to protect it.

4.1.2 Reviewing and Understanding OPIC Information Security Policies

This section of the Handbook provides information and instructions for Information Owners on fulfilling your security responsibilities.

You should also take the opportunity to review the Information Systems Security Program (ISSP) Directive and detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have any questions, please ask the ISSO to provide clarification.

4.2 Classifying Resources

For more information on resource classification, see OPIC ISSP-02, *Information Resource Classification*.

All OPIC resources must be classified based on their sensitivity and criticality so that they may be appropriately protected commensurate with their level of classification. As the assigned owner of an OPIC information resource, you are responsible for performing this classification in accordance with the OPIC information classification framework. The ISSO will be available to assist you with this process.

4.3 Assigning An Information Custodian

Although you are the official owner of an information resource, you do not have to personally manage and operate that resource. Although the requirements for an information resource (and the usage of the resource) often come from OPIC business units, it is more appropriate that the actual installation, maintenance, and administration of that resource be performed by someone with specialized expertise in performing those tasks. Therefore, you can delegate that role onto another individual or group, such as IRM.

The person who is responsible for managing and maintaining the resource is called an "Information Custodian." As the resource owner, you are responsible for making an arrangement with someone who will assume this custodian role. (At OPIC, this will generally be the IRM department.) A Service Level Agreement should be developed between the owner and custodian outlining roles, responsibilities, and expectations.

Please note that while the information custodian will assume the day-to-day responsibilities for operating and maintaining the resource, and will assist the owner with planning for and implementing security measures, it is the information owner for the resource who is ultimately responsible for the security of that resource.

4.4 Risk Management

For more information on Risk Management, see OPIC ISSP-03, *Risk Management*.

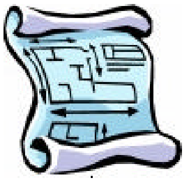
In determining an information security strategy for a system or the organization, OPIC must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns.

Risk management (RM) is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel. Effective RM processes support sound *risk-based decision-making*. The CIO and other OPIC executives need to ensure implementation of an effective and comprehensive RM program which encompasses all segments of the enterprise in order to support OPIC's mission.

As an information owner, you are expected to use a risk-based approach to making decisions regarding the acquisition and protection of your information resources. Risk analysis will determine requirements that ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, OPIC information. You are responsible for performing periodic risk assessments of your resources and implementing appropriate safeguards based on these analyses. These analyses and safeguards will be documented in system security plans.

4.5 Developing System Security Plans

For more information on System Security Plans, see OPIC ISSP-07, *System Security Plans*.



A System Security Plan (SSP) lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures. The System Security Plan will be used as a critical component of the Certification and Accreditation of the system, which is required by FISMA and enforced by OMB.

As an information owner, you are responsible for ensuring that SSPs are developed for each major system that you own, and you must formally approve and accept these plans. As part of this process, you are to ensure that:

- Each system is fully documented.
- MOUs are in place for connections to other systems.
- Sufficient and appropriate measures are implemented to protect OPIC resources.

Each System Security Plan must be reviewed, updated, and re-approved at least once every two years, or when there is a major change to the system, whichever happens first.

SSPs must be marked, handled, and controlled as sensitive but unclassified information.

4.6 Vulnerability Testing

For more information on vulnerability testing, see OPIC ISSP-09, *Vulnerability Testing*

Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand information security attacks.

Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires OPIC to perform penetration and vulnerability testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist OPIC with determining its information security priorities and making prudent investments to enhance the security posture of its information resources.

The ISSO will develop a program to perform periodic, standardized vulnerability testing of all OPIC systems. Attempts will be made to minimize disruption of business operations.

As the owner of an OPIC information system, it is your responsibility to:

- Cooperate with, and provide assistance as requested to, the ISSO and other designated personnel for performing testing on your systems.
- Provide information required to perform testing
- Support and participate in development of testing “rules of engagement”.
- Resolve vulnerabilities discovered by testing, as reported in the test results.
- Document steps taken to resolve vulnerabilities and report these to the ISSO.

4.7 Certifying & Accrediting Your Systems

For more information on C&A, see OPIC ISSP-08, *Certification and Accreditation*.

Certification and Accreditation (C&A) is used 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 three years or when there is a change that affects the system's security posture.

If you are the owner of a major OPIC information system[2], then you are responsible for certifying and accrediting your system in accordance with the following requirements:

- You will submit your system for evaluation at least every three years or whenever there is a major change to the security of the system (whichever happens first). Upon publication of this Handbook, existing operational systems that have not been certified and accredited within the last 3 years shall undergo Certification and Accreditation within 1 year. All new OPIC IT systems will be certified and accredited prior to being allowed into operation.
- Certification shall not only address software and hardware security safeguards, but also procedures, physical protections, and personnel security measures.
- Security Testing & Evaluation (ST&E) will be performed during Certification to evaluate the effectiveness of security measures implemented for the system.
- You must meet the following minimum requirements for your system to receive certification:
  - The system must be thoroughly documented (to NIST standards).
  - A system security plan (see section 4.5) must be developed and approved.
  - 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.
  - A risk assessment must be conducted.
  - The findings of the ST&E must be resolved (via mitigation, transference, or acceptance of the risks).
- Accreditation will be in the form of a formal declaration by the Designated Approving Authority (DAA) that the resource is approved to operate in a particular security mode using a prescribed set of safeguards. An Accreditation statement will be used to declare that proper attention has been afforded to the security of the resource. The statement shall address the residual risks associated with the respective system or network, subsequent to the implementation of countermeasures

[2] A major information system is one that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

applied during the system test and evaluation.

- The Accreditation determination shall be based on findings, facts, and support documents produced during the Certification process, as well as other management considerations.
- You will review the Certification and Accreditation statements before they are signed by the DAA.
- You must notify the ISSO when there is a significant change to the security of any major information system that you own.

4.8 Contingency Planning

For more information on Contingency Planning, see OPIC ISSP-10, *Contingency Planning.*

In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice, and part of the fundamental mission of OPIC as a responsible and reliable public institution. For the success of OPIC's programs, the agency's information systems must be available or recoverable in the event of disruptions.

OPIC's information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of OPIC's risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside OPIC's control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus, effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

As an information owner, you are responsible for the development of a Contingency Plan, Continuity of Support Plan, or Disaster Recovery Plan for each major information system that you own. These plans will be based on a business impact analysis, and will identify measures to reduce the effects of system disruptions and increase system availability. Recovery strategies and procedures will be developed to ensure that systems may be recovered quickly and effectively following a disruption. Testing will occur annually or when a significant change occurs. Contingency plans will be reviewed regularly and updated as needed to remain current.

4.9 System Development

Security must be treated as an integral part of any system development or implementation project, including system modifications. It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later. By considering security early in the system life cycle, OPIC will be able to avoid higher costs later on while also developing a more secure system from the start.

4.9.1 Software Development Life Cycle (SDLC)

For more information on system development security requirements, see OPIC ISSP-28, *System Development*.

Each information system passes through multiple phases during its lifetime as it is planned, developed, deployed, operated, and retired. In order to develop a secure system in a cost effective manner, certain security-related activities must be performed during each of these phases. You are responsible not only for ensuring that the required tasks are completed during the development/acquisition cycle for the systems that you own, but you must actively participate in all phases to that the system is secure and meets your requirements.

1. Initiation Phase:

   (a) Conduct sensitivity assessment (taking into account information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, and OPIC policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (*e.g.*, hazardous location) and public threats to the system or information should also be considered.

   (b) Perform preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

2. Development/Acquisition Phase:

   (a) Security requirements shall be developed at the same time system planners define the other requirements of the system.

   (b) The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.

   (c) Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.

   (d) A System Security Plan (SSP) is to be developed in accordance with OPIC System Security Plan policy and procedures.

   (e) Operational practices will be developed, including standard operational procedures and system-specific security policies (*e.g.*, account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.

3. Implementation Phase:

   (a) The system's security features will be configured and enabled.

   (b) The system's security management procedures will be implemented.

(c) The system will be tested and authorized for processing via OPIC's Certification and Accreditation (C&A) process.

4. Operation/Maintenance Phase:

   (a) The security activities outlined in the system security plan (*e.g.*, performing backups, holding training classes, managing accounts) will be performed.

   (b) Any changes made, or maintenance performed, on the system are to comply with OPIC's Change Control and Patch Management policies and processes.

   (c) Periodic security audits and vulnerability tests will be performed in accordance with OPIC Audit and Vulnerability Testing policies.

5. Disposal Phase:

   (a) Information may be moved to another system, archived, discarded or destroyed in accordance with OPIC data retention policies.

   (b) Any storage media must be disposed of in accordance with OPIC's Media Management policies.

   (c) The disposition of software needs to be in keeping with its license or other vendor agreements

4.9.2 What Security Requirements Must Be Met By All New Systems/Applications?

In addition to the SDLC requirements, all systems that are developed or acquired must meet the following requirements:

- Each application must be categorized in accordance with OPIC's Information Resource Classification policy, and provided protection appropriate to its level of sensitivity and criticality.
- Systems must be thoroughly tested prior to placing them in the OPIC production operating environment.
- Do not use sensitive data to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.
- Any hardware and software used at OPIC must be obtained through authorized procurement channels and must comply with all licensing requirements.
- Systems must comply with all OPIC information security policies and procedures (*e.g.*, system hardening, access control, backup, password policies, etc.)

4.10 Protecting Your Data

For more information on database security, see OPIC ISSP-30, *Database Security*

OPIC has been entrusted with a variety of sensitive data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this data. To protect this information, OPIC must implement data security measures, such as validation and verification controls. These controls are used to prevent accidental or malicious data alteration or destruction, and to assure that data meets quality expectations.

As an Information Owner, you are responsible for:

- Ensuring the confidentiality, integrity, and availability of the data that you own.
- Authorizing and limiting access to the data that you own.
- Reporting data security incidents to the ISSO.

Additionally, you must ensure that data repositories comply with the following:

- Data will be secured commensurate with its level of sensitivity and criticality.
- Databases, and applications that interface with databases, will be configured in accordance with security best practices:
  - Integrity verification tools, such as consistency and reasonableness checks, will be used to look for evidence of data tampering, errors and omissions.
  - Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure that software and data have not been modified.
  - If users are allowed to make updates to a database via a web page, these updates must be validated to ensure that they are warranted and safe.
  - Table access controls will be applied to databases containing sensitive data. Access to specific data within the database will be limited to only those personnel who need access, and will be limited to only those functions (*e.g.*, read, modify) required for the person to perform his or her duties.
  - Database servers must only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).
  - For sensitive data, audit trails must be created and maintained within the database to track transactions and provide accountability.
  - Selectively encrypting data within the database in order to protect sensitive information is highly encouraged.
- Programs or utilities that may be used to maintain and/or modify sensitive databases or software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully tested, selected, and controlled.
- Never put databases containing non-public information on the same physical machine as a public web server.
- Data repositories (and database servers) that store public information cannot be used to also store non-public (*e.g.*, private, proprietary, sensitive) information.
- Database servers and database software must adhere to all OPIC information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

4.11 Server Security

For more information on servers, see OPIC ISSP-21, *Server Security*.

It takes only one incorrectly configured system to allow an intruder into OPIC's network. Therefore, no server should ever be placed on the network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

If you are the owner of any OPIC server, or of an application that has a dedicated server, then you are responsible for complying with the following server security requirements:

- For each server that you own, you must apply the OPIC standard base security configuration for that type of server, or ensure that the configuration is applied by the custodian.
- The level of security applied to each server will be appropriate to the level of criticality and sensitivity of the data and services that the server provides.
- System patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures. Logs must be kept documenting the updates that have been installed on each server, including at minimum the name of the server, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.
- Unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).
- Access to the server must be controlled in accordance with the OPIC Access Control and Identification and Authentication policies.
- Auditing and logging will be enabled on the server in accordance with OPIC auditing policies and procedures.
- Antivirus software will be installed, maintained, and configured on the server in accordance with OPIC antivirus policies and procedures.
- An approved warning banner, which specifies requirements and penalties for accessing the server, will be provided upon access to the server
- The server will be inventoried and tracked in accordance with OPIC asset management policies and procedures.
- The configuration and purpose of the server will be thoroughly documented, and the currentness of this documentation will be maintained.
- Any changes made to the configuration of the server will be performed in accordance with OPIC change management policies and procedures.
- The server will be housed in an approved, access-controlled and environmentally protected location, in accordance with OPIC physical and environmental security policies and procedures.

4.12 Authorizing Access Permissions

For more information, see OPIC ISSP-11, *Access Control* and OPIC ISSP-16, *Personnel Security.*

For information on background investigations, contact the OPIC Security Officer.

Excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability. Therefore, access to OPIC information resources is limited to those who need those resources to perform their duties. Access to specific resources is only to be granted to authorized personnel who have a legitimate need to use them, and will be limited to those privileges required for their duties.

As an information owner, you are responsible for determining who will have access to your resource, and the level of access granted. In making this determination, you are to adhere to the following policies:

- Ensure that your resources are protected against unauthorized access by implementing appropriate access control measures.
- Access is only to be granted to personnel who have a legitimate business need.
- Grant users only the minimum access permissions required for their duties.
- Users must have appropriate clearance for the sensitivity level of the resources to which they are given access. Prior to granting someone access to sensitive information resources, you must verify that they have undergone the appropriate background investigation and that it has resulted in a suitable outcome.
- Use a documented process for granting, modifying, and revoking permissions.
- Before granting contractors or other non-OPIC personnel access to any sensitive data, you must make sure that they have signed a nondisclosure agreement.
- Periodically review access permissions and make adjustments as appropriate.

4.13 Identifying and Authenticating Users

For More Information, see OPIC ISSP-12, *Identification and Authentication* and ISSP-32, *Password Management.*

In order to ensure that unauthorized persons do not have access to sensitive OPIC information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access controls can then be used to allow or limit access based on the established user identity.

The specific method(s) of authentication used for each system shall be appropriate to the level of sensitivity of the system (*i.e.*, more sensitive systems should use stronger authentication methods). Multiple authentication methods (*e.g.*, use of both a password and a token) may be required for high-sensitivity resources or high-risk situations.

As an Information Owner, you must ensure that access to your information resource(s) is protected by ensuring that any passwords used for authentication are properly assigned and protected. In order for passwords to be an effective tool for providing security, they must be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

You must ensure that passwords are appropriately assigned, used, and managed on the resources that you own, and that password and authentication policies are enforced. When feasible, automated techniques should be used for enforcement (*e.g.*, configure the system to only accept passwords that meet specific policy criteria.)

4.14 Maintaining Audit Trails

For more information on audit trails, see OPIC ISSP-13, *Audit Trails*.

In order to enforce information security policies, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be maintained. This is used to investigate security incidents, monitor use of OPIC resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

As an Information Owner, you must ensure that your systems comply with OPIC audit trail policies by meeting the following requirements:

- For each server, you must enable and maintain logs for the following:
  - Server startup and shutdown
  - Loading and unloading of services
  - Installation and removal of software
  - System alerts and error messages
  - User logon and logoff
  - System administration activities
  - Accesses to sensitive information and systems
  - Modifications of privileges and access controls
  - Additional security related events
- For each major application, you must enable and maintain logs for the following:
  - Modifications to the application
  - Application alerts and error messages
  - User sign on and sign off
  - System administration activities
  - Accesses to sensitive information
  - Modifications of privileges and access controls
- For each for each router, firewall, or other major network device that you own, you must enable and maintain logs for at least the following transactions:
  - Device startup and shutdown
  - Administrator logon and logoff
  - Configuration changes
  - Account creation, modification, or deletion
  - Modifications of privileges and access controls
  - System alerts and error messages
- For each logged transaction, you must record the type of event, date, time, and the name of the account performing the transaction.
- Do not store sensitive information, such as passwords and system data, in the logs.

- Cooperate with and provide assistance (as requested) to the ISSO and other designated personnel, who will perform periodic audits of the log files to look for potential security issues or to research an incident.
- Ensure that only approved, designated personnel have access to the audit logs so that they will be protected from tampering.
- All audit trail files are to be kept for at least 1 year and stored in a secure location. Audit trails associated with known incidents (including those used for legal action) are to be kept for 3 years.

4.15 Backup & Recovery

For more information on media management, see OPIC ISSP-19, *Backup and Recovery*.

There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include such events as hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at OPIC.

It is therefore essential that OPIC maintain backup copies of all critical data and systems so that they can be used to ensure the continued availability and viability of these resources when these unfortunate events occur. The action of copying (or mirroring) important data to a second location or onto removable media is calling “backing up.”

As the owner of an OPIC resource, it is your responsibility to make sure that your resource is successfully backed up in accordance with OPIC policies. This means working with your Information Custodian to ensure that the following requirements are met:

- You must back up all critical OPIC information resources that you own.
- Critical data and system configurations must be backed up on at least a daily basis.
- Applications and licenses will be backed up whenever there are changes to them.
- You will send backups to an approved, environmentally-controlled, off-site storage location at least 30 miles from the OPIC office.
- You will define and implement a backup retention schedule for your resources which complies with OPIC’s data retention policies.
- You will develop and implement detailed procedures for performing backups restoring data, testing backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.
- You will periodically test your back up and restore procedures to ensure that data can be effectively restored from the backups.
- You will be treat backups with the same level of criticality and sensitivity as the data and applications stored on them.
- Persons who have access to the backups, or who have access to perform backup or restore functions, must undergo appropriate background screening in accordance with OPIC Personnel Security policy prior to being given such access.
- You will handle backup tapes in accordance with OPIC Media Management policy.

4.16 Managing System Changes

For more information on change management, see OPIC ISSP-18, *Change Control*.

Changes to OPIC's information systems must be controlled and managed to ensure integrity of the system and its data. OPIC information systems require appropriate administrative, physical and technical controls to be incorporated into both new additions and changes to systems. These controls must encompass not only the software, but also the routine activities that enable OPIC's information systems to function properly (*e.g.*, fixing software or hardware problems, loading and maintaining software, updating hardware and software, and maintaining a historical record of changes). Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure, and other problems.

As an Information Owner, you are responsible for ensuring that changes made to your resources are documented and implemented in compliance with OPIC policy:

- Changes will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.
- OPIC will develop baseline information that includes a current list of all components (hardware, software, and their documentation), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.
- For each of your systems, OPIC will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.
- Procedures will be implemented to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:
  - Establish who performs maintenance and repair activities.
  - Contain procedures for performance of emergency repair and maintenance.
  - Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.
- Impact analyses will be conducted to determine the effect of proposed changes on existing systems and security controls.
- Standardized procedures will be implemented for thoroughly testing and approving system components (operating system, other system, utility, applications) and configuration changes prior to transition from development to production.
- Information Users will be notified regarding how they will be impacted by changes.
- Current backups will be available when changes are made.
- All software, operating systems, and patches shall be installed in accordance with U.S. copyright regulations, the license for that software, and OPIC policies.
- Only authorized personnel may make changes to OPIC information systems.
- Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.
- Change control documentation (especially change logs) will be available even if the network is down and will not contain passwords for affected components.

4.17 Patches & System Updates

For More Information, see OPIC ISSP-20, *Patch Management & System Updates.*

Maintained patch levels are critical to the security of OPIC systems. Vendors will typically provide patches and fixes for security problems, which can be loaded separately from the application or operating system. These should be loaded on a regular basis using a coordinated process.

As the owner of any OPIC information resource, it is your responsible to make sure that patches and system updates are applied to your resource in a timely and coordinated manner (usually by the custodian) in accordance with the following requirements:

- During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency situation (such as an ongoing security incident), more urgent (perhaps immediate) application of new security patches may be required.
- Check patches for compatibility with all system components prior to applying them.
- Test patches on non-production systems prior to loading them on production systems.
- Patching should be performed during scheduled maintenance, except in emergencies.
- Back up systems prior to installing new patches.
- Maintain a log book for each system, which records the status and configuration of the system. Information to be recorded includes: date of the action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator remarks.

4.18 Media Management

For more information on media management, see OPIC ISSP-31, *Media Management.*

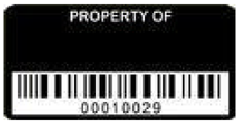
OPIC has been entrusted with a variety of sensitive data in order to accomplish its mission. This data, which is stored on a variety of media (*e.g.*, hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes), must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, OPIC uses a variety of security mechanisms that provide protections for media.

As an Information Owner, you are responsible for the proper handling and disposal of your media in accordance with OPIC policies and procedures. This includes:

- Provide appropriate physical and environmental protections for stored media.
- Mark any media containing sensitive data with its classification level. Labeling shall include any special handling instructions.
- Media containing sensitive data must be secured (*e.g.*, in locked drawer, cabinet or safe) when not in use or unattended. Media containing sensitive data transported through the mail or by courier service shall be double-sealed. The second envelope shall be appropriately marked with the sensitivity classification of the data.
- Monitor the receipt and delivery of media containing sensitive data, and account for media to ensure that data is not lost and potentially compromised while in transit.
- Sanitize (*i.e.*, securely delete) media that contain sensitive data before disposal, in accordance with OPIC media sanitization procedures.
- Report the loss, damage, or theft of any media entrusted to you to the ISSO.

4.19 Asset Management

For more information on asset management, see OPIC ISSP-33, *Asset Management*.



Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the unwanted attention of auditing organizations like GAO and OMB.

Not only would loss of information assets result in a financial impact on OPIC, but it could also result in unauthorized access to data stored on, or accessed by, these assets, and could have a detrimental effect on the image and reputation of the agency. Additionally, several federal laws and regulations, such as the Clinger-Cohen Act, mandate the tracking and management of information assets.

As an information owner, you are responsible for inventorying, tracking, and protecting the assets that you own. This includes ensuring that the following tasks are performed:

- Keep a record of all information assets that you own, including, but not limited to, workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.
- You are to record and barcode your information assets upon receipt at OPIC.
- For each information asset, you must track the following information:
  - The brand, model, and type of asset
  - Serial number and OPIC barcode
  - The person to whom the asset is assigned
  - The location of the asset
  - Any maintenance agreements for the asset
  - The date of receipt of the item
  - The date that the record was last updated or inventoried
- Upon disposal of an information asset, you must track the date of disposal, the method of disposal (*e.g.*, transfer, destruction, donation, etc.), and the name of the new owner (if there is one).
- You are required to perform periodic inventories to verify your records and account for all information assets. Each asset is to be inventoried at least annually.

4.20 Physical & Environmental Security

For more information on physical security, see OPIC ISSP-17, *Physical and Environmental Security.*

Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

As the owner of an information resource, you must ensure that your resource is located in an area which meets the following standards:

- Physical access to information resources is to be controlled commensurate with the classification of the resource and the level of risk.
- Areas containing sensitive information resources require special restrictions to limit access to these resources:
  - Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
  - Personnel without an appropriate security clearance must be escorted.
  - Areas containing sensitive information must be physically secured in accordance with OPIC facility security policies and OPIC Directive 94-14.
  - Access history data (*i.e.*, logs) will be maintained.
- Areas containing critical information resources require special protections to safeguard the availability of these resources:
  - Implement protections against fire, flood, electromagnetic disturbance, humidity, and other environmental factors that could damage the resources.
  - Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
  - Smoke and fire detection systems with alarms must be installed in accordance with OPIC Physical and Environmental security policies.
- Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. Keep backups in a separate location from originals.

If you are the owner of the Computer Room (*i.e.*, "Data Center"), you must comply with the following requirements:

- Meet all requirements listed above.
- Install fire suppression equipment and provide fireproof storage.
- Provide emergency power shutdown controls. Cover them to prevent accidental activation.
- Equipment is to be located on a raised floor.
- Provide an uninterruptible power supply.
- Vendors and visitors are to be escorted at all times.
- All physical access to the room must be tracked.
- Annual testing will be performed on all fire, utility, and environmental alarms and protective systems.

4.21 Security Training & Awareness

For more information on security training, see OPIC ISSP-04, *Security Training and Awareness.*

As the owner of an information resource, it is your responsibility to ensure that users of your system are trained on and aware of the specific security policies and procedures that apply to your system. These policies and procedures should be documented and published for your users, and training provided if necessary.

4.22 Incident Reporting

For more information on incident reporting, see OPIC ISSP-05, *Incident Reporting*.

You must immediately report any suspected information security incidents so that OPIC may respond in a timely manner to minimize disruption of critical information services and minimize loss or theft of sensitive and mission-critical information.

As an information owner, you may receive reports from users or the information custodian regarding security incidents involving your resources. You may also personally discover such incidents. In either case, you are obligated to report these incidents to the ISSO using OPIC's incident reporting process.

4.23 Incident Response

For more information on incident response, see OPIC ISSP-06, *Incident Response*.

OPIC 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.

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.

As an information owner, it is your responsibility to cooperate and support OPIC's incident response procedures. Such cooperation will make it possible for OPIC to respond quickly and effectively to situations that might compromise the agency's information resources.

Specifically, your responsibilities include:

- Ensuring that incident response procedures are in place for your resources
- Providing a report to the ISSO within one working day after the incident. Critical incidents must be reported immediately.
- Cooperating with, and providing assistance as requested to, the ISSO or other designated personnel investigating an incident on any of the resources you own.
- Informing OPIC management of significant incidents (*e.g.,* major compromise of data, denial of service).
- Implementing additional measures, as needed, to prevent further incidents.
- Providing follow up to ensure that incidents have been resolved.

4.24 Virus Protection

For more information on the virus protection, see OPIC ISSP-14, *Antivirus*.

The use of antivirus software is essential for protecting OPIC resources from the danger posed by computer viruses and other malicious programs.

If you are the owner of any OPIC server, workstation, laptop, or email gateway, you are responsible for ensuring that the resource is running agency standard, supported antivirus software, and that the software is updated automatically as new virus profiles are made available by the vendor. The antivirus software must be configured to quarantine or delete infected files that cannot be repaired, and to scan all portable media before it is used on the computer. Furthermore, any infected resources that cannot be cleaned by the antivirus software must be removed from the OPIC network.

In the rare event that lab testing conflicts with antivirus software, run the antivirus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the antivirus software is disabled, do not run any applications that could transfer a virus (*e.g.*, email or file sharing).

4.25 Using Encryption

For more information on the encryption, see OPIC ISSP-15, *Encryption*.

Encryption is an important tool that can be used to protect the confidentiality and integrity of information. It is OPIC's policy that proven, government-approved encryption technologies be used to protect sensitive information which is transferred or stored outside of the OPIC computing environment (*i.e.* on traveling laptops or for transmission over the Internet). This use must adhere to the following policies:

- The use of encryption to protect sensitive data, both in storage and in transmission, is encouraged.
- Only government-approved encryption techniques and devices may be used.
  - All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.
  - Digital certificates used or issued by OPIC will comply with the Federal Public Key Infrastructure.
- 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.
- OPIC will obey all regulations regarding restrictions on export of encryption technologies.
- You 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.
- Any encryption solution used must have a process for the ISSO to perform administrative recovery of lost keys.
- Any use of digital certificates to provide non-repudiation must be approved by the ISSO and Legal Affairs.

4.26 Telephone Equipment

For more information on telephony, see OPIC ISSP-26, *Telephony Security*.

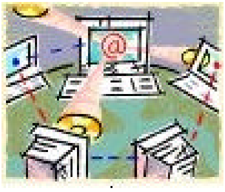
Telephone services are intended to support the objectives and operations of OPIC, and are critical to fulfilling OPIC's mission. However, these telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.

As an owner of a telephony resource, or of a system that uses telephony resources, you are responsible for deploying, managing, and protecting the telephony resources in compliance with OPIC information security policies, including the following:

- The agency PBX and other critical telephony components must be stored in a secure, environmentally controlled location in accordance with OPIC physical security policy.
- Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.
- Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.
- Modems or other telephony equipment may not be installed without the explicit approval of the appropriate official (*e.g.*, OPIC Telecommunications Officer for telephone equipment, or Director of Technical Services for modems and related telephony equipment).
- As a rule, the following applies to requests for fax and analog lines:
  - Fax lines are to be approved for departmental use only. No fax lines will be installed for personal use.
  - Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.
  - Waivers for the preceding policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request. (See OPIC ISSP-26, Telephony Security for more information.)
- The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within OPIC will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency, and active penetrations have been launched against such lines by hackers. Waivers to the policy will be granted on a case-by-case basis (See OPIC ISSP-26, Telephony Security for more information.)
- Any connectivity between the telephone system and the OPIC network (OPICNET) must be approved by the Director of Technical Services and the ISSO.

4.27 Network Security

For more information on network security, see OPIC ISSP-23, *Network Security*.



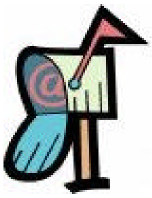
It takes only one incorrectly configured system to allow an intruder into OPIC's network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.

If you are the owner of a network device, then you are responsible for adhering to the following requirements:

- Standard base security configurations will be applied to each type of network component (*i.e.* routers, switches, etc.)
- The level of security applied to each network component will be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.
- Patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures. Logs must be kept documenting the patches and updates that have been installed on each device, including at minimum the name of the device, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.
- Any unnecessary services will be disabled. (For example, if a router does not need to be managed by SNMP, then SNMP should be disabled.)
- Access to all OPIC network devices must adhere to the OPIC Access Control and Identification and Authentication policies.
- Remote administration of network devices can only be performed using encrypted and authenticated connections.
- Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.
- Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.
- Each device must be inventoried and tracked in accordance with OPIC asset management policies and procedures.
- Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a device must be performed in accordance with OPIC change management policies and procedures.
- Network devices will be located in access-controlled and environmentally-protected facilities, in accordance with OPIC physical and environmental security policies and procedures.
- No device may be connected to the OPIC network without approval from the Director of Technical Services.

4.28 Electronic Mail

For more information on electronic mail security, see OPIC ISSP-29, *Electronic Mail*.



Electronic mail is an essential tool used by OPIC to conduct its business. However, email is inherently insecure and presents many risks to OPIC information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to OPIC resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

If you are the owner of a resource (including a device or application) that provides or uses electronic mail services, you must abide by the following rules:

- All electronic mail services provided on OPICNET must be approved by the Director of Technical Services. This includes the use of SMTP or other protocols or services by an application/system.
- All incoming electronic mail must be scanned and filtered for viruses, disallowed content (including certain types of attachments), and other potentially malicious content.
- Sensitive information may not be sent over any public network (*e.g.*, the Internet) unless it is encrypted.
- Electronic mail systems must adhere to and support OPIC record retention policies. This includes periodic archival and deletion of messages.

4.29 Remote Access

For more information on remote access, see OPIC ISSP-25, *Remote Access*

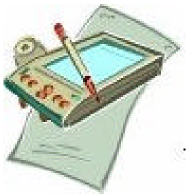
Remote access to OPICNET provides many benefits. It allows personnel traveling on business to connect to OPIC information resources and provides the capability for telecommuting. However, remote access to OPIC via dial-up or other connectivity poses a risk of intrusion into OPICNET by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of OPICNET also lacks the protections afforded by OPIC's corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.

As the owner of a resource which provides remote access into the OPIC computing environment, you are responsible for ensuring that the following requirements are met for your resource:

- Any remote access into the OPIC computing environment must be approved by the Director of Technical Services.
- All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).
- All sensitive data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
- All security policies used in the OPIC office must also be observed when using or connecting to OPIC resources while outside the OPIC office environment.

4.30 Mobile Devices

For more information on mobile device security, see OPIC ISSP-22, *Mobile Computing*.



The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow OPIC personnel to be more productive. However, the use of these devices outside of the OPIC office poses risks to those devices and the information they contain. These devices may also present a hazard to other OPIC resources upon their return to the OPIC office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of OPICNET which lack the protections afforded by OPIC's corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.

If you are the owner of any mobile devices, you are responsible for complying with the following requirements:

- Laptops and other mobile computing devices must be inventoried and tracked.
- Laptops must have antivirus software installed and enabled.
- Laptops should have personal firewall software installed and enabled when the laptop is used outside of the OPIC environment.
- Any mobile device (e.g., a laptop or PDA) which stores or transmits sensitive data, or which can be used to connect to other sensitive OPIC systems, should require users to authenticate (*i.e.*, logon) in order to gain access.
- If the device is used to store sensitive data, then encryption or other appropriate measures must be deployed to protect this data.
- The loss, theft, or destruction of any mobile device must be immediately reported to the ISSO.

4.31 Wireless Networking

For more information on wireless, see OPIC ISSP-27, *Wireless Security*.

In addition to the risks that apply to all networks, wireless connectivity has additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to OPIC networks via the hijacked device. Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

As the owner of any wireless resource, you have the following infosec responsibilities:

- The use of any wireless connectivity or device for accessing or transmitting OPIC information must be approved by the Director of Technical Services, regardless of whether these devices are owned by OPIC.
- You must use OPIC Risk Management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that you own.

- All OPIC wireless devices must be labeled and inventoried.
- Access to OPIC and other systems and networks must be immediately terminated for any lost or stolen devices.
- Access to any OPIC systems or networks using wireless devices or wireless networks must be authenticated.
- Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems.
- Ongoing, randomly timed security audits should be used to monitor and track wireless and handheld devices.
- Patches and security enhancements must be applied to wireless networks in accordance with OPIC system security policy.
- Robust cryptography (at least 128bit) must be used whenever sensitive data is stored or transmitted on a wireless device.
- The SSID for each device should be configured such that it does not reveal any identifying information about OPIC.
- Inherent security features such as authentication and encryption methods that are available in wireless technologies should be tested and used.
- You must communicate the specific policies and procedures for securely using your wireless resources to the users of those resources.

4.32 Perimeter Protection

Any connectivity to systems or networks outside of OPIC provides an opening for unauthorized personnel to access or tamper with OPIC information resources. Such threats range from intruders breaking into OPIC's network to steal or alter data to service disruptions propagated from other systems. OPIC must implement firewalls and other precautions to prevent, detect, and resolve incidents arising from these threats.

4.32.1 What Must OPIC Do To Protect The Agency's Computing Perimeter?

For more information on perimeter protection, see OPIC ISSP-24, *Perimeter Protection.*

There are certain security protections that must be implemented at the enterprise level to protect OPIC's information resources. If you are the information owner for OPIC's general enterprise computing environment (*i.e.*, OPICNET), then you are responsible for implementing and managing appropriate perimeter protections as prescribed by OPIC ISSP-24, *Perimeter Protection.* These requirements include, but are not limited to:

- Use of firewall and intrusion detection systems configured to security best practices.
- Creation of a DMZ for placement of web-facing systems and services to protect the internal OPIC network.
- Use of a proxy server for all outbound connections to the Internet from the internal OPIC network.
- Formalization of Network Trust Relationships between OPICNET and external networks (such as those of other agencies) to which OPIC is connected.

4.32.2 What Are The Responsibilities Of Someone Who Owns A Resource That Resides Or Provides Services At The Perimeter?

If you are the owner of any resource that resides on, or provides services at, the perimeter of the OPIC network (*e.g.*, Internet web servers), you are responsible for ensuring that your resources comply with the following requirements:

- These systems must be placed in a protected DMZ.
- No sensitive data is to be stored on systems located in the DMZ. All sensitive data must be located within the internal network. Waivers may be granted as needed.
- Access from the Internet to these systems must not make sensitive information or information systems vulnerable to compromise (*i.e.*, these systems cannot be used to compromise other internal systems).
- All perimeter equipment must be documented in accordance with OPIC information system documentation procedures.
- The use of any of the following services on DMZ systems and perimeter systems, and the permitting of these services into OPICNET from external sources, must be approved by the ISSO: HTTP, FTP, Telnet, Finger, WHOIS, Gopher, SSL, SQL, RSH, NNTP, TN3270, Rlogin, POP3, and streaming media.
- All hardware and software deployed on the perimeter must adhere to OPIC system security policies and procedures, including the disabling of all unnecessary services.
- Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to OPIC change control procedures.
- All security related events on perimeter equipment, as well as access to OPICNET via this equipment, must be logged and audited in accordance with OPIC's Audit Trail policies and procedures.
- The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures must be documented. COTRs are responsible for third party compliance with this policy.

4.32.3 What Are The Requirements For Connectivity To Other Networks Or External Systems (Such As Those At Other Agencies)?

If your system needs connectivity to another system or external network (other than the Internet), then the connection must comply with the following criteria:

- All connections between OPICNET and external networks (such as those of other agencies) must be approved by the Director of Technical Services.
- Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.
- An interconnection security agreement will be developed and signed by OPIC and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.
- All connections to external networks will pass through OPIC approved firewalls.
- Information Owners will validate the need for all such connections annually.

SECTION 5:

GUIDE FOR INFORMATION CUSTODIANS

5.1 Understanding And Accepting Your Security Responsibilities

An important aspect of OPIC's Information Systems Security Program (ISSP) is ensuring that everyone understands and accepts their individual security responsibilities. Only by making personnel aware of their security responsibilities and teaching them correct practices can OPIC reduce the level of security risk to its information systems.

Many components of OPIC's ISSP are aimed at improving your awareness of the need to protect system resources; developing your skills and knowledge so that you may perform your job more securely; and building individual accountability into OPIC's program. Ensuring that you gain an understanding of your responsibilities is vital to OPIC because without your knowing the necessary security measures (and to how to use them), OPIC's information security will not be effective.

As someone who has been assigned duties related to the development, implementation, maintenance, or administration of an OPIC information resource, you are an "Information Custodian." As such, you have specific information security responsibilities. You are responsible for familiarizing yourself with and performing these responsibilities as outlined in this Handbook.

5.1.1 Signing The Elevated Privileges/ Information Custodian Agreement

For more information on the Information Custodian Agreement, see OPIC ISSP-04, *Security Training and Awareness.*

In order to perform their duties, information custodians are usually assigned additional access privileges on the resources for which they have been assigned custodianship. These privileges come with additional responsibilities for safeguarding your access credentials and using them appropriately. Misuse of your elevated privileges, or failure to protect them from disclosure, can seriously impact the security of OPIC information resources.

In order to be granted administrative privileges, you must sign an agreement acknowledging that you understand the additional responsibilities and agree to use the privileges only for the purposes for which they have been granted. A signed copy of the agreement (see ISSP – 04 in the appendices) must be provided to the ISSO.

5.1.2 What Security Responsibilities Does An Information Custodian Have?

As an information custodian, you have direct impact on the security of OPIC resources because you are the one who implements and operates the security controls that have been prescribed for the resources that you manage. Your responsibilities include the following duties, which are described later in this section:

- Assisting the information owner with planning safeguards to protect the resource and to ensure compliance with all OPIC information security policies.
- Implementing and operating the safeguards for the resource.
- Assisting the ISSO with auditing resources under your management and investigating security incidents which affect those resources, as requested.
- Immediately reporting incidents that occur on your resources to the ISSO.
- Maintaining thorough, up-to-date documentation on your resources.
- Adhering to all OPIC information security standards and procedures for administration and maintenance of the resource (*e.g.*, change control, backups, etc.)
- Assist with recovery of resource functionality and integrity in the event of disaster.

5.1.3 Reviewing And Understanding OPIC Information Security Policies

This section of the Handbook provides information and instructions for Information Custodians on fulfilling your information security responsibilities

You should also take the opportunity to review the Information Systems Security Program (ISSP) Directive and detailed Information Security Policies (ISPs) provided in the appendices of this Handbook.

It is your responsibility to make sure you read and *understand* these policies and procedures. If you have any questions, please ask your supervisor or the ISSO to provide clarification.

5.2 Developing System Security Plans

For more information on System Security Plans, see OPIC ISSP-07, *System Security Plans*.

A System Security Plan (SSP) lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures. The System Security Plan will be used as a critical component of the Certification and Accreditation of the system.

As an information custodian, you will be called upon to assist the owner of each major system that you manage with developing an SSP. As part of this process, you will fully document the configuration of the system, and help the owner to determine appropriate security measures to protect the system. Each System Security Plan must be reviewed, updated, and re-approved at least once every two years, or when there is a major change to the system, whichever happens first.

SSPs must be marked, handled, and controlled as sensitive but unclassified information.

5.3 Certifying & Accrediting Systems

For more information on C&A, see OPIC ISSP-08, *Certification and Accreditation.*

Certification and Accreditation (C&A) is used 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 three years or when there is a change that affects the system's security posture.

If you are the custodian of a major OPIC information system, then you will assist the owner of the system with certifying and accrediting that system. You may also be called upon by the ISSO to assist with security testing of the system during the C&A process.

5.4 Contingency Planning

For more information on Contingency Planning, see OPIC ISSP-10, *Contingency Planning.*

In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice, and part of the fundamental mission of OPIC as a responsible and reliable public institution. For the success of OPIC's mission, the agency's information systems must be available in the event of disruptions.

OPIC's information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, managerial, or operational solutions as part of OPIC's risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside OPIC's control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus, effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

If you are the custodian of a major OPIC information system, then you are responsible for the assisting the owner of that system with the development of a Contingency Plan, Continuity of Support Plan, or Disaster Recovery Plan. These plans will be based on a business impact analysis, and will identify measures to reduce the effects of system disruptions and increase system availability. You will help develop recovery strategies and procedures to ensure that systems may be recovered quickly and effectively following a disruption, and will participate in testing of the plans annually or when a significant change occurs. Additionally, you will assist with reviewing the plans regularly and updating them as needed to remain current.

5.5 Vulnerability Testing

For more information on vulnerability testing, see OPIC ISSP-09, *Vulnerability Testing.*

Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand security attacks.

Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires OPIC to perform security testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist OPIC with determining its security priorities and making prudent investments to enhance the security posture of its information resources.

The ISSO will develop a program to perform periodic, standardized vulnerability testing of all OPIC systems. Attempts will be made to minimize disruption of business operations.

As the custodian of an OPIC information resource, it is your responsibility to:

- Cooperate with, and provide assistance as requested to, the ISSO and other designated personnel for performing testing on your systems.
- Resolve vulnerabilities discovered by testing, as reported in the test results.
- Document steps taken to resolve vulnerabilities and report these to the ISSO.

5.6 System Development

Security must be treated as an integral part of any system development or implementation project, including system modifications. It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on. By considering information security early in the system life cycle, OPIC will be able to avoid higher costs later on while also developing a more secure system from the start.

5.6.1 Software Development Life Cycle (SDLC)

For more information on system development security requirements, see OPIC ISSP-28, *System Development.*

Each information system passes through multiple phases during its lifetime as it is planned, developed, deployed, operated, and retired. In order to develop a secure system in a cost effective manner, certain security-related activities must be performed during each of these phases. You are responsible for ensuring that the required tasks are completed during the development/acquisition cycle for the systems that you own:

1. Initiation Phase:

   (a) Conduct sensitivity assessment (taking into account information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, and OPIC policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (*e.g.*, hazardous location) and public threats to the system or information should also be considered.

   (b) Perform preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

2. Development/Acquisition Phase:

   (a) Security requirements shall be developed at the same time system planners define the other requirements of the system.

   (b) The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.

   (c) Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.

   (d) A System Security Plan (SSP) is to be developed in accordance with OPIC System Security Plan policy and procedures.

   (e) Operational practices will be developed, including standard operational procedures and system-specific security policies (*e.g.*, account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.

3. Implementation Phase:

   (a) The system's security features will be configured and enabled.

   (b) The system's security management procedures will be implemented.

   (c) The system will be tested and authorized for processing via OPIC's Certification and Accreditation (C&A) process.

4. Operation/Maintenance Phase:

   (a) The security activities outlined in the system security plan (*e.g.*, performing backups, holding training classes, managing accounts) will be performed.

   (b) Any changes made, or maintenance performed, on the system are to comply with OPIC's Change Control and Patch Management policies and processes.

   (c) Periodic security audits and vulnerability tests will be performed in accordance with OPIC Audit and Vulnerability Testing policies.

5. Disposal Phase:

   (a) Information may be moved to another system, archived, discarded or destroyed in accordance with OPIC data retention policies.

   (b) Any storage media must be disposed of in accordance with OPIC's Media Management policies.

   (c) The disposition of software needs to be in keeping with its license or other agreements

As an information custodian, your primary duties will occur in the Operation/Maintenance phase. However, you may play an important role in many of the activities that occur in the other phases. In particular, you are likely to be responsible for the following:

- Assisting the information owner with design, technical reviews, and requirements development. You are to consider security throughout these activities.
- Assisting the information owner with developing a System Security Plan, as well as system-specific security policies and procedures.
- Implementing and testing technical and procedural security controls for the system.
- Assisting with Certification & Accreditation of the system.
- Performing security and maintenance tasks on the system in accordance with OPIC policies.
- Securely disposing of system components in accordance with OPIC policies upon retirement of the system.

5.7 Protecting Your Data

For more information on database security, see OPIC ISSP-30, *Database Security*.

OPIC has been entrusted with a variety of sensitive data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this information. In order to protect the data, OPIC must implement data security measures, such as data validation and verification controls. These controls are used to protect data from accidental or malicious alteration or destruction, to provide assurance that the information meets the expectations about its quality, and to ensure that it has not been altered.

As an Information Custodian, you are responsible for:

- Assisting Information Owners with maintaining the confidentiality, integrity, and availability of their data.
- Assisting Information Owners with implementing database security controls.
- Immediately reporting database security breaches to the data owner and the ISSO.

Additionally, you must ensure that data repositories that you manage are compliant with the following security requirements:

- Data will be secured commensurate with its level of sensitivity and criticality.
- Databases, and applications that interface with databases, will be configured in accordance with security best practices:
    - Integrity verification programs, such as consistency checks, shall be used to look for evidence of data tampering, errors, and omissions.
    - Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure that software and data have not been modified.
    - If users are allowed to make updates to a database via a web page, these updates must be validated to ensure that they are warranted and safe.
    - For databases containing sensitive information, table access controls will be applied. Access to specific information within the database will be limited to only those personnel who need access to that information, and access will be limited to only those functions (*e.g.*, read, write, modify, etc.) required for the person to perform his or her duties.
    - Database servers must be configured to only allow connections from authorized, trusted sources (such as web servers to which they supply data).
    - For sensitive data, audit trails must be created and maintained within the database to track transactions and provide accountability.
    - You are encouraged to selectively encrypt data within the database in order to protect sensitive information.
- Programs or utilities that may be used to maintain and/or modify sensitive databases and other software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully controlled.
- Databases containing non-public information should never be on the same physical machine as a web server.
- Data repositories (and database servers) that store public information cannot be used

to also store non-public (*e.g.*, private, proprietary, sensitive) information.

- Database servers and database software must adhere to all OPIC information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

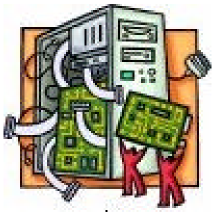
5.8 Server Security

For more information on server security, see OPIC ISSP-21, *Server Security*.

It takes only one incorrectly configured system to allow an intruder into OPIC's network. Therefore, no server should ever be placed on the network without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

If you are the custodian of any OPIC server, then you are responsible for complying with the following server security requirements:

- Standard base security configurations will be applied to all servers.
- The level of security applied to each server will be commensurate with the level of criticality and sensitivity of the data and services that it provides.
- System patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures. Logs must be kept documenting the updates that have been installed on each server, including at minimum the name of the server, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.
- Any unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).
- Access to all OPIC servers must adhere to the OPIC Access Control and Identification and Authentication policies.
- Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.
- All servers must run antivirus software configured in accordance with OPIC antivirus policies and procedures.
- Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.
- Each server must be inventoried and tracked in accordance with OPIC asset management policies and procedures.
- Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a server must be performed in accordance with OPIC change management policies and procedures.
- Servers will be located in access-controlled and environmentally protected facilities, in accordance with OPIC physical and environmental security policies and procedures.



5.9 Managing Access Permissions

For more information on assigning access permissions, see OPIC ISSP-11, *Access Control*.

Access to OPIC information resources is only to be granted to authorized personnel who have a legitimate need to use them, and access privileges for each resource will be limited to only those required to perform their duties. Excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting them.

As an information custodian, you are responsible for administering access permissions for the resources you manage, based on direction from the information owner. You are to work with the owner to develop and implement a process for managing access which complies with the following policies:

- Ensure that your resources are protected against unauthorized access.
- Use a documented process for granting, modifying, and revoking permissions.
- Grant access only to personnel who have a legitimate business need.
- Grant each user only the minimum access permissions required for their duties.
- Prior to granting someone access to sensitive information, verify that they have passed the appropriate background investigation.
- Before granting contractors or other non-OPIC personnel access to any sensitive data, make sure that they have been authorized by their COTR or VP for this access.
- Periodically review access permissions and make adjustments as appropriate.

5.10 Identification & Authentication

For More Information, see OPIC ISSP-12, *Identification and Authentication* and ISSP-32, *Password Management*.

In order to ensure that unauthorized persons do not have access to sensitive OPIC information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access can then be granted based on established identity.

The specific method(s) of authentication used for each resource shall be appropriate to its level of sensitivity (*i.e.*, more sensitive systems require stronger authentication). Multiple methods (*e.g.*, use of both a password and a token) may be required in high-risk situations.

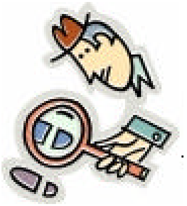
If passwords are used for authentication, it is critical that they be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

Information custodians are responsible for:

- Assisting owners with determining and implementing appropriate authentication measures for their resources.
- Ensuring that passwords are appropriately assigned, used, and managed on the resources you manage, and that password and authentication policies are enforced. When feasible, automated techniques should be used to ensure strong passwords.
- Instructing users on the specific password and logon policies of the resource.
- Reporting password or account compromises to the ISSO and information owner.

5.11 Maintaining Audit Trails

For more information on audit trails, see OPIC ISSP-13, *Audit Trails*.



In order to enforce information security policies, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or “audit trail”) of system and application processes and user activity of systems and applications must be kept.

As an information custodian, you are responsible for configuring and maintaining audit trails on the resources that you manage, in accordance with the following requirements:

- For each server, you must enable and maintain logs for the following transactions:
  - Server startup and shutdown
  - Loading and unloading of services
  - Installation and removal of software
  - System alerts and error messages
  - User logon and logoff
  - System administration activities
  - Accesses to sensitive information and systems
  - Modifications of privileges and access controls
  - Additional security related events
- For each major application, you must enable and maintain logs for the following transactions:
  - Modifications to the application
  - Application alerts and error messages
  - User sign on and sign off
  - System administration activities
  - Accesses to sensitive information
  - Modifications of privileges and access controls
- For each for each router, firewall, or other major network device that you manage, you must enable and maintain logs for the following transactions:
  - Device startup and shutdown
  - Administrator logon and logoff
  - Configuration changes
  - Account creation, modification, or deletion
  - Modifications of privileges and access controls
  - System alerts and error messages
- For each logged transaction, you must record the type of event, date, time, and the name of the account performing the transaction.

- Do not store sensitive information, such as passwords and system data, in the logs.
- Cooperate with and provide assistance (as requested) to the ISSO and other designated personnel, who will perform periodic audits of the log files to look for potential security issues or to research an incident.
- Control access to the audit logs to prevent tampering.
- Keep all audit trail files for at least one year and store them in a secure location. Audit trails associated with known incidents (including those used for legal action) are to be kept for three years.

5.12 Backup & Recovery

For more information on media management, see OPIC ISSP-19, *Backup and Recovery*.

There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include, but are not limited to, hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. It is therefore essential that OPIC maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.

As the custodian of an OPIC resource it is your responsibility to successfully back up your resources in accordance with OPIC policies, which include:

- You must back up all critical OPIC information resources that you manage.
- Back up critical data and system configurations on at least a daily basis.
- Back up applications and licenses whenever there are changes to them.
- Send backups to an approved, environmentally-controlled, off-site storage location at least 30 miles from the OPIC office.
- Define and implement a backup retention schedule for your resources which complies with OPIC's data retention policies.
- Develop and implement detailed procedures for performing backups, restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.
- Periodically test your back up and restore procedures to ensure that data can be effectively restored from the backups.
- Handle backups with the same criticality and sensitivity as the data and applications stored on them, and in accordance with OPIC Media Management policy.
- Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with OPIC Personnel Security policy prior to being given such access.

5.13 Security Training & Awareness

For more information on security training, see OPIC ISSP-04, *Security Training & Awareness.*

As the custodian of an information resource, it is your responsibility to train users, and make them aware of, the specific security policies and procedures of your system. These policies and procedures should be documented and published, and training provided if necessary.

5.14 Managing System Changes

For more information on change management, see OPIC ISSP-18, *Change Control*.

Changes to OPIC's information systems must be controlled and managed to ensure integrity of the system and its data. OPIC information systems require appropriate administrative, physical and technical controls to be incorporated into both new additions and changes to systems. These controls must encompass not only the software, but also the routine activities that enable OPIC's information systems to function properly (*e.g.*, fixing software or hardware problems, loading and maintaining software, updating hardware and software, and maintaining a historical record of application changes). Change control prevents unexpected changes from inadvertently causing denial of service, unauthorized disclosure of information, and other problems.

As an Information Custodian, you are responsible for implementing and documenting changes to your systems in compliance with OPIC policies and procedures:

- You will systematically plan, obtain approval, test and document changes to each system.
- You will develop baseline information that includes a current list of all components (hardware, software, and their documentation), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings, for your systems.
- For each of your information systems, you will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.
- You will implement procedures to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:
  - Establish who performs maintenance and repair activities.
  - Provide for emergency repair and maintenance contingencies.
  - Ensure compliance with hardware/software warranties.
  - Procedures for verifying system and data integrity once change is complete.
- You will maintain version control that associates system components to the appropriate system version.
- You will conduct impact analyses to determine the effect of proposed changes on existing systems and security controls.

- You will implement procedures for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.
- You will adequately notify users regarding how they will be impacted by changes.
- You will have current backups available when changes are made.
- You will install all software, operating systems, and patches in accordance with U.S. copyright regulations, the license for that software, and applicable OPIC Information Security policies.
- You will only make changes to OPIC information systems for which you are authorized to do so.
- You will document the change control procedures for your systems to provide a complete audit trail of decisions and design modifications.
- You will keep change control documentation (especially change logs) available even if the network is down.

5.15 Patches & System Updates

For More Information, see OPIC ISSP-20, *Patch Management & System Updates.*

Maintained patch levels are critical to the security of OPIC systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a regular basis using a coordinated process.

As the custodian of any OPIC information resource, it is your responsible to apply patches and system updates in a timely and coordinated manner. Specifically, you must adhere to the following requirements:

- During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency situation (such as an ongoing security incident), more urgent application of new security patches may be required.
- Patches will be checked for compatibility with all system components prior to being applied.
- Patches will be successfully tested on non-production systems prior to being loaded on production systems.
- Patching should be performed during an authorized outage window unless there is an urgent situation that is approved by the DTS or ISSO.
- Systems will be backed up prior to installation of new patches.
- All OPIC systems will have a log book. System log books help record the status of network equipment and provide continuity among administrators. The log book may be in paper or electronic form. Information to be recorded includes: date of the action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator remarks.

5.16 Media Management

For more information on media management, see OPIC ISSP-31, *Media Management*.

OPIC has been entrusted with a variety of sensitive data in order to accomplish its mission. This data, which is stored on a variety of media (*e.g.*, hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes), must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, OPIC uses a variety of security mechanisms that provide protections for media.

Information custodians are responsible for the proper handling of media that has been entrusted to them, in accordance with OPIC policies and procedures. This includes:

- Providing appropriate physical and environmental protections for stored media.
- Marking any media containing sensitive data with its classification level. Labeling shall include any special handling instructions.
- Securing any media containing sensitive data (*e.g.*, storing it in a locked drawer, cabinet, or safe) when not in use or unattended. Any media containing sensitive information transported through the mail or courier/messenger service shall be double-sealed. The second envelope shall be appropriately marked with the sensitivity classification of the data.
- Monitoring the receipt and delivery of media containing sensitive data, and accounting for the media to ensure that data is not lost and potentially compromised while in transit.
- Sanitizing media that contains sensitive data before disposal, in accordance with OPIC media sanitization procedures.
- Reporting (to the information owner and the ISSO) the loss, damage, or theft of any media that has been entrusted to you.

5.17 Virus Protection

For more information on the virus protection, see OPIC ISSP-14, *Antivirus*.

The use of antivirus software is essential for protecting OPIC resources from the danger posed by computer viruses and other malicious programs.

If you are the custodian of any OPIC server, workstation, laptop, or email gateway, you are responsible for installing and managing standard, supported antivirus software on that resource, and ensuring that the software is updated automatically as new virus profiles are made available by the vendor. The antivirus software must be configured to quarantine or delete infected files that cannot be repaired, and to scan all portable media before it is used on the computer. Furthermore, any infected information resources that cannot be cleaned by the antivirus software must be removed from the OPIC network until they can be verified as virus free.

If lab testing conflicts with antivirus software, run the antivirus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the antivirus software is disabled, do not run any applications that could transfer a virus, *e.g.*, email or file sharing.

5.18 Asset Management

For more information on asset management, see OPIC ISSP-33, *Asset Management*.

Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations like GAO and OMB.

Not only would loss of information assets result in a financial impact on OPIC, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, several federal laws and regulations, such as the Clinger-Cohen Act, mandate the tracking and management of information assets.

Information custodians are responsible for assisting information owners with inventorying, tracking, and protecting the information assets which they own. This includes performing the following tasks:

- Keeping a record of all information assets under their custodianship, including, but not limited to, workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.
- Information assets are to be added to the record upon receipt by OPIC and assigned a barcode.
- For each information asset, track at least the following information:
  - The brand, model, and type of asset
  - Serial number and OPIC barcode
  - The person to whom the asset is assigned
  - The location of the asset
  - Any maintenance agreements for the asset
  - The date of receipt of the item
  - Date the record was last updated or inventoried
- Upon disposal of an information asset, track the date of disposal, the method of disposal (*e.g.*, transfer, destruction, donation, etc.), and the name of the new owner.
- Perform periodic inventories to verify records and account for all information assets. Each asset is to be inventoried at least annually.

5.19 Telephone Equipment

For more information on telephony, see OPIC ISSP-26, *Telephone Security*.

Telephone services are intended to support the objectives and operations of OPIC, and are critical to fulfilling OPIC's mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.

As a custodian of a telephony resources, you are responsible for assisting information owners with deploying, managing, and protecting their telephony resources in compliance with OPIC information security policies. (See section 4.27.)

5.20 Incident Reporting

For more information on incident reporting, see OPIC ISSP-05, *Incident Reporting*.

You must immediately report any suspected information security incidents so that OPIC may respond in a timely manner to minimize disruption of critical information services, as well as to minimize the loss or theft of sensitive and mission-critical information.

As an information custodian, you may receive reports from users or the information owner regarding security incidents involving your resources. You may also personally discover such incidents. In either case, you are obligated to report these incidents to the ISSO using OPIC's incident reporting process, and to inform the information owner.

5.21 Incident Response

For more information on incident response, see OPIC ISSP-06, *Incident Response*.

The 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.

Additionally, 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 organizations to have an incident response capability and to share information concerning common vulnerabilities and threats.

As an information custodian, it is your responsibility to cooperate with and support OPIC's incident response procedures. Such cooperation will make it possible for OPIC to respond quickly and effectively to situations that might compromise the agency's information resources.

Specifically, your responsibilities include:

- Implementing incident response procedures for your resources.
- Providing a report to the ISSO within one working day after the incident. Critical incidents must be reported immediately.
- Documenting incidents and the resolution steps that were taken.
- Cooperating with, and providing assistance as requested to, the ISSO or other designated personnel investigating an incident on any of the resources for which you are the custodian.
- Informing the information owner regarding incidents.
- Implementing additional measures, as needed, to prevent further incidents.
- Providing follow up to ensure that incidents have been resolved.

5.22 Using Encryption

For more information on encryption, see OPIC ISSP-15, *Encryption*.

Encryption is an important tool that can be used to protect the confidentiality and integrity of information. OPIC's policy is that proven, government-approved encryption technologies be used to protect sensitive information which is transferred or stored outside of the OPIC computing environment (*e.g.*, on traveling laptops or for transmission over the Internet). This use must adhere to the following policies:

- The use of encryption to protect sensitive data, both in storage and in transmission, is encouraged.
- Only government-approved encryption techniques and devices may be used.
  - All encryption products must be Federal Information Processing Standard (FIPS) 140-2 or 197 certified.
  - Digital certificates used or issued by OPIC will comply with the Federal Public Key Infrastructure.
- The use of proprietary encryption algorithms is not allowed, unless reviewed by qualified experts outside of the vendor and approved by the DTS and ISSO.
- Obey all regulations regarding restrictions on export of encryption technologies.
- Procedures must be documented and implemented for managing encryption keys, in order to ensure that these keys are protected from unauthorized disclosure, destruction, or misuse.
- A process must exist that allows the ISSO to administratively recover lost keys.
- Any use of digital certificates to provide non-repudiation must be approved by the ISSO and Legal Affairs.

5.23 Electronic Mail

For more information on electronic mail, see OPIC ISSP-29, *Electronic Mail*.

Electronic mail is an essential tool used by OPIC to conduct its business. However, email is inherently insecure and presents many risks to OPIC information. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to OPIC resources. Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.

If you are the custodian of a resource that provides or uses electronic mail services, you must abide by the following rules:

- All electronic mail services provided on the OPIC network (OPICNET) must be approved by the Director of Technical Services. This includes the use of SMTP or other protocols or services (including relays) by an application or system.
- All incoming email must be scanned and filtered for viruses, disallowed content (including certain types of attachments), and other potentially malicious content.
- Sensitive information may not be sent over any public network (*e.g.*, the Internet) unless it is encrypted.
- Electronic mail systems must adhere to and support OPIC record retention policies. This includes periodic archival and deletion of messages.

5.24 Network Security

For more information on network security, see OPIC ISSP-24, *Network Security*.

It takes only one incorrectly configured system to allow an intruder into OPIC's network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.

If you are the custodian of a network device, then you are responsible for assisting the owner of the resource with implementing and managing security for that resource, and adhering to the following requirements:

- Standard base security configurations will be applied to each type of network component (*i.e.* routers, switches, etc.)
- The level of security applied to each network component will be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.
- Patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures. Logs must be kept documenting the patches and updates that have been installed on each device, including at minimum the name of the device, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.
- Any unnecessary services will be disabled (*e.g.*, if a router does not need to be managed by SNMP, then SNMP should be disabled).
- Access to all OPIC network devices must adhere to the OPIC Access Control and Identification and Authentication policies.
- Remote administration of network devices can only be performed using encrypted and authenticated connections, and must be approved by the DTS and ISSO.
- Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.
- Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network, device, or application.
- Each device must be inventoried and tracked in accordance with OPIC asset management policies and procedures.
- Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.
- Any changes made to the configuration of a device must be performed in accordance with OPIC change management policies and procedures.
- Network devices will be located in access-controlled and environmentally-protected facilities, in accordance with OPIC physical and environmental security policies.
- No device may be connected to the OPIC network without approval from the DTS.

5.25 Remote Access

For more information on remote access, see OPIC ISSP-25, *Remote Access*.

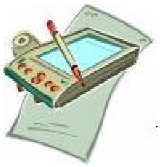
Remote access to OPICNET provides many benefits. It allows personnel traveling on business to connect to OPIC information resources and provides the capability for telecommuting. However, remote access to OPIC via dial-up or other connectivity poses a risk of intrusion into OPICNET by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of OPICNET also lacks the protections afforded by OPIC's corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.

As the custodian of a resource which provides remote access into the OPIC environment, you are responsible for assisting the resource owner with the following requirements:

- Any remote access into the OPIC computing environment must be approved by the Director of Technical Services.
- All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).
- All sensitive data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.
- All security policies for use in the OPIC office environment must also be observed when using or connecting to OPIC resources while outside the OPIC office.

5.26 Mobile Devices

For more information on mobile devices, see OPIC ISSP-22, *Mobile Computing*.



The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow OPIC personnel to be more productive. However, the use of these devices outside of the OPIC office poses risks to those devices and the information they contain. These devices may also present a hazard to other OPIC resources upon their return to the OPIC office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of OPICNET which lack the protections afforded by OPIC's corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.

If you are the custodian of any mobile devices, then you are responsible for assisting the owner of these resources with complying with the following requirements:

- Laptops and other mobile computing devices must be inventoried and tracked.
- Laptops must have antivirus software installed and enabled.
- Laptops should have personal firewall software installed and enabled when the laptop is used outside of the OPIC environment.
- Access to mobile devices which store or transmit sensitive data, or which can be used to connect to other sensitive OPIC systems, must be authenticated.
- If the device is used to store sensitive data, then encryption or other appropriate measures must be deployed to protect this data.
- The loss, theft, or destruction of any mobile device must be immediately reported to the ISSO and the DTS.

5.27 Wireless Networking

For more information on wireless networking, see OPIC ISSP-27, *Wireless Security*.

In addition to the risks that apply to all networks, wireless connectivity is exposed to additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tied up network bandwidth and denied service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to OPIC networks via the hijacked device. Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

As the custodian of any wireless connectivity resource, you have the following responsibilities regarding wireless security:

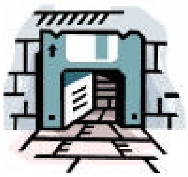
- Assisting the owner of the resource with planning, implementing, and managing security controls to safeguard the wireless resource and the data transmitted over it. (See section 4.26.)
- Safeguarding wireless information resources with which you have been entrusted.
- Adhering to OPIC policies and procedures for the administration of wireless devices, including:
  - Labeling all wireless devices prior to deployment.
  - Maintaining an inventory of all wireless devices.
- Disabling access or service for wireless devices that have been lost or stolen.
- Obtaining permission from the Director of Technical Services before using or installing any wireless network cards, routers, or access points on OPICNET.

5.28 Perimeter Protection

For more information on perimeter protection, see OPIC ISSP-24, *Perimeter Security*.

Any connectivity to systems or organizations outside of OPIC provides an opening for unauthorized personnel to access or tamper with OPIC information resources. Such threats range from intruders breaking into OPIC's network to steal or alter data to service disruptions propagated from other systems. OPIC must implement firewalls, intrusion detection systems, and other precautions to prevent, detect, and resolve incidents arising from these threats.

As an information custodian, you are responsible for assisting information owners with deploying and managing perimeter resources and associated security measures, and complying with OPIC perimeter protection policies. (See section 4.29 for details.)



5.29 Physical Security

For more information on physical security, see OPIC ISSP-17, *Physical and Environmental Security*.

Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

As the custodian of an information resource, you must implement and operate physical and environmental protections for your resource which meet the following standards:

- Physical access is to be controlled according to the sensitivity of the resource.
- Areas containing sensitive resources require special restrictions to limit access:
  - Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.
  - Personnel without an appropriate security clearance must be escorted.
  - Areas containing sensitive information must be physically secured in accordance with OPIC facility security policies and OPIC Directive 94-14.
- Critical resources require special protections to safeguard their availability:
  - Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.
  - Automated systems should monitor for environmental problems and alert specified personnel as appropriate.
- Smoke and fire detection systems with alarms must be installed in accordance with OPIC Physical and Environmental security policies.
- Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals, not only for damage considerations, but also to guard against thefts.

If you are the custodian of the Computer Room (*i.e.*, “Data Center”), you must:

- Meet all requirements listed above.
- Install fire suppression equipment.
- Provide emergency power shutdown controls.
- Locate equipment on a raised floor.
- Provide an uninterruptible power supply.
- Escort vendors and visitors at all times.
- Track all physical access to the room.
- Perform annual testing on fire, utility, and environmental alarms and systems.

APPENDIX A: OPIC INFORMATION SYSTEMS SECURITY DIRECTIVE

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 adequa te 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 informatio n 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.

APPENDIX B: OPIC INFORMATION SYSTEMS SECURITY POLICIES

Overseas Private Investment Corporation

Information Resources Management

INFORMATION SECURITY POLICIES & PROCEDURES

October 2004

TABLE OF CONTENTS

1 INTRODUCTION

Information is critical to performing OPIC's mission. OPIC information, in all its forms and throughout its life cycle, must be protected through information management policies and actions that meet applicable federal regulatory requirements and support the agency's mission, vision, and values. Measures must be taken to protect OPIC's information resour ces from unauthorized modification, disclosure, or destruction, whether accidental or intentional.

"The possibility that electronic information could be lost, corrupted, diverted, or misused represents a real threat to mission performance for … government agencies… [OPIC has become dependent upon information technology as an essential resource for performing its mission.] "However, even as … dependence on information technology has grown, so too has the vulnerability of this technology and the range of external threats to it…

IT resources also consume a growing share of the Federal budget and are becoming increasingly important to daily life. As a result, a considerable body of applicable policy is in place, consisting of laws, statutes, regulations, Executive Orders, and other directives. [OPIC's] IT Security Program, as well as those of other agencies, must operate within this complex policy landscape to ensure that the Government meets its obligations to the Nation. Providing for the security of IT resources is not only a difficult technical challenge, it is also a human challenge. Ultimately IT security is a human endeavor that depends heavily on the behavior of individual people."[1]

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 unclassified information systems. As part of the ISSP, there must be explicit and well-defined security policies that establish requirements for minimum safeguards, assign roles and responsibilities, provide accountability, and address penalties for noncompliance.

"Information security investment is pointless without an effective policy. Organizations must adopt a structured framework for policy definition using an inclusive policy management process that enables policies derived from business requirements… Failure to develop a meaningful security policy that maps to business risk seriously compromises the ability to develop effective security solutions and could expose the organization to potentially catastrophic breaches."[2]

[1] Adopted from the Introduction to the *GSA Security Action Plan*

[2] META Group, *Making Information Policy Effective*, July 2002

This enterprise information security policy document describes the policies, standards, guidelines, and procedures that OPIC will follow to safeguard its information resources and ensure consistency with government-wide policies and standards.

2 OBJECTIVES

The purpose of this information security policy document is to identify and disseminate the principles and framework that guide the secure use of information usage at OPIC. Specifically, this document discusses:

- The principles that guide implementation of the information security program at OPIC
- Federal regulations and standards with which OPIC must comply
- OPIC business-driven security requirements
- The information security policy framework to be used at OPIC
- The set of OPIC information security policies

3 SCOPE

The policies in this document define the minimum set of security requirements for protecting OPIC's information systems and complying with applicable regulations.

These policies cover the use of unclassified systems and information only. Classified information may not be created, transmitted, or stored on any computer that is connected to the OPIC network. Policies governing security of classified information are provided in Management Directive 94-14, *OPIC Security Program*.

OPIC information security policies apply to everyone who uses or has access to OPIC's information assets, including employees, contractors, clients, vendors, and visitors. All of these personnel are responsible for understanding and complying with these policies.

4 GUIDING PRINCIPLES

The development of OPIC's information security policies is driven by the following principles:

- OPIC must fully comply with all applicable regulations and federal guidelines regarding information security.
- OPIC's information resources are critical to its business and worth protecting.
- Information security should support OPIC's mission and business needs.
- OPIC is committed to protecting the private information entrusted to the agency by its customers and business partners.
- Information security is an essential component of sound IT management.
- OPIC's security program will focus on managing risk effectively and cost efficiently by employing industry best practices.
- Information security is the responsibility of all OPIC information users and can only be successfully achieved through communication and cooperation.
- OPIC's information security policies, procedures, and guidelines should be periodically reassessed to ensure continued effectiveness.
- A comprehensive and integrated approach is required to provide effective information assurance.
- OPIC would like to develop a reputation as an information security role model for other small government agencies.

5 REQUIREMENTS

As a federal government corporation, OPIC is in a unique situation. As a corporation, OPIC faces similar security threats, and has similar security requirements, to any financial corporation. At the same time, OPIC faces the additional security threats and requirements that apply to federal agencies. OPIC must protect client information, employee data, proprietary business information, and its own corporate assets as any corporation would, while also meeting federal government information security mandates such as FISMA, OMB requirements, and presidential directives. Therefore, OPIC's information security program, and the policies that guide it, must address both the business and government agency aspects of OPIC's security needs. The following sections will discuss each of these sets of requirements. The combined set of these requirements forms the basis for OPIC's information security policies.

5.A Federal Government Requirements

OPIC is subject to a variety of federal security requirements, including government regulations, federal standards, and the mandates of oversight agencies. These include, but are not limited to, the following, which are described in detail in Appendix A:

- Federal Information Security Management Act of 2002 (FISMA)
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, *Security of Federal Automated Information Resources*
- Homeland Security Presidential Directive 7, *Critical Infrastructure Protection*
- OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies
- OMB Memo M-99-20, Security of Federal Automated Information Resources
- Privacy Act of 1974, as amended
- Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.
- Clinger-Cohen Act of 1996
- Computer Abuse Amendments Act of 1994
- Computer Security Act of 1987, PL 100-235, January 8, 1988.
- Computer Fraud and Abuse Act of 1986
- National Institute of Standards and Technology (NIST) Guidance

5.B OPIC Business Requirements

"The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets… Security, therefore, is a means to an end and not an end in itself. To act on this, managers need to understand both their organizational mission and how each information system supports that mission. After a system's role has been defined, the security requirements implicit in that role can be defined. Security can then be explicitly stated in terms of the organization's mission."[3]

5.B.I Agency Description

OPIC is an independent agency of the Federal government. The agency is contained on four floors of a commercial building leased from a private landlord in downtown Washington, DC. OPIC's network operations and computer room are located onsite. The agency staff of approximately 230 is predominated by investment officers, and also includes associated support personnel (*e.g.*, legal, administrative, physical security, information resources and human resources personnel). Approximately 38 onsite contractors supplement agency staff. The agency has a telecommuting program, and a handful of OPIC employees work from international remote offices (*e.g.*, in Turkey and in Russia).

OPIC's mission is to mobilize and facilitate the participation of United States private capital and skills in the economic and social development of less developed countries and areas, and countries in transition from non-market to market economies, thereby complementing the development assistance objectives of the United States.[4] In accomplishing its mission, OPIC promotes positive U.S. effects and host country developmental effects. OPIC assures that the projects it supports are consistent with sound environmental and worker rights standards. In conducting its programs, OPIC also takes into account guidance from the Administration and Congress on a country's observance of, and respect for, human rights. In accomplishing its mission, OPIC operates on a self-sustaining basis.

[3] NIST Special Publication 800-12 "An Introduction to Computer Security: The NIST Handbook", p. 11

[4] 22 U.S.C. §2191

5.B.II OPIC Business Environment

OPIC's central IT needs are based on its mission of providing political risk insurance to help U.S companies manage risk; providing financing through direct loans and loan guaranties; and leveraging private capital through OPIC-supported funds.

OPIC's business environment is transactional and information-driven. Unlike other Federal agencies that provide direct services to the American public (*e.g.*, issuing Social Security checks, controlling air traffic, or providing healthcare to veterans), OPIC's customer is the American business or investor seeking long-term investment financing or insurance. OPIC's due diligence and clearance processes, the key processes leading up to finance, insurance and investment funds transactions, require analysis of sensitive company, project and country-specific information and can sometimes span months. OPIC's small business center considers applications in a 60-day streamlined process in order to meet the unique needs of small and medium-sized enterprises.

To accomplish its mission, OPIC requires continuous operation during business hours of several key systems or applications, including the OPIC network (OPICNET), Oracle Government Financials, and a number of external systems that support cash flow and payroll operations. OPIC's intranet is important to the daily operation of the Corporation since this aspect of the network supplies access to agency information, policies, electronic forms, administrative applications (such as timekeeping), and interoffice communications.

5.B.III Critical Information Assets

OPIC has many critical assets to protect, including:

- Personnel – regular government employees, contractors, consultants, interns, etc.
- Property – facilities and office space, physical plant, furniture, etc.
- Data / Information – vital records, sensitive and protected information, etc.
- Equipment – hardware, infrastructure, mobile devices, etc.
- Software – desktop/network software, business applications, data management software, etc.

All of these assets are vital to the continued operational viability and success of OPIC.

Of particular interest to the OPIC Information Security Program is the security and viability of OPIC's critical data and information assets, which include the following categories:

- ❖ **Program and Legal Information** is essential for OPIC to carry out its programmatic and legal functions and activities and to protect the U.S. government and the legal and financial rights of OPIC's clients. Examples include client information;

Finance/Insurance/Investment Funds case file information; working documents; bilateral agreement information; and FOIA information.

- ❖ **Financial Information** is essential for OPIC to carry out its financial functions and activities. Examples include accounts payable/receivable information; fixed assets, general ledger, and subsidy information; portfolio information; budget and travel information.

- ❖ **Administrative Information** is used by OPIC to effectively meet its mission requirements in compliance with existing laws, rules and regulations. Examples include interagency agreements; strategic plans and business plans; management directives and administrative orders; and procurement information.

- ❖ **Personnel Information** is necessary for OPIC to administer human resources programs, including compensation and benefits. Examples include payroll information; benefits information; retirement information; time and attendance information; and program information (*e.g.*, staffing, employee relations, etc.).

- ❖ **Corporate Governance Information** represents the thinking behind OPIC's major mission and policy decisions and program direction. Examples include the OPIC charter and by-laws; Board briefing books and notational votes; Board meeting minutes; Board resolutions; and Investment Committee proceedings.

- ❖ **Emergency Operating Information** is essential to the continued function or reconstitution of OPIC during and after an emergency. Examples include continuity of operations plan; orders of succession; disaster recovery plan; vital records manual; and building plans.

- ❖ **Library Resources** are both sources and compilations of information that enable OPIC's departments to conduct their due diligence for OPIC projects. Examples include financial data and analyses; political information; sector analyses; credit reports of companies; country information; and legal information.

- ❖ **Information From Other Federal Agencies** is information that OPIC is privy to in order to carry out its duties to support the goals of the Administration. Examples include White House guidance; travel itineraries; and strategic information.

5.B.IV Areas of Risk

"Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity. The effects of various threats vary considerably: some affect the confidentiality or integrity of data while others affect the availability of a system."[5] Table 5-1 shows the potential harm or damage that could result from threats to OPIC's critical information systems:

Table 5-1: Potential Risks to OPIC Information Resources

Critical Information Resource	Potential Harm or Damage
Program and Legal Information	Legal and Financial Liability; Disclosure of Sensitive/Client Confidential Data; Loss of Client Confidence; Inability to Perform Mission
Financial Information	Financial loss or Loss of Assets; Disclosure of Sensitive Data; Inability to Perform Mission; Closer Scrutiny by OMB and Congress
Administrative Information	Inability to Perform Mission (Effectively); Disclosure of Sensitive Data
Personnel Information	Financial or Legal Liability; Disclosure of Privacy Act protected information; Loss of Employee Confidence; Closer Scrutiny by OPM
Corporate Governance Information	Financial or Legal Liability; Loss of Client Confidence; Disclosure of Sensitive Information
Emergency Operating Information	Disclosure of Sensitive Information; Inability to Perform Mission
Library Resources	Disclosure of Sensitive Data
Information From Other Federal Agencies	Disclosure of Sensitive Data; Loss of Other Agency Confidence

The primary goal of the OPIC Information Security Program is to mitigate these threats and vulnerabilities by preventing them or reducing their impact when they occur. Without a comprehensive security program, customized to OPIC's specific needs and environment, OPIC is exposed and vulnerable to losing its ability to perform its mission, and may risk liability for not protecting the resources with which it has been entrusted.

[5] NIST Special Publication 800-12 "An Introduction to Computer Security: The NIST Handbook", p. 25

OPIC needs to understand the risks and vulnerabilities of its information resources in order to apply cost effective measures to protect them. This section provides a general description of the risks that threaten OPIC’s information resources. This information can then be used to determine the information security policies that are needed by OPIC.

OPIC faces a variety information security threats, ranging from terrorist acts to employee theft to accidental exposure/alteration of data. Inherent vulnerabilities also exist in the corporate assets themselves. Figure 5-1 illustrates some of the threats that exist to OPIC information systems. Each of these threats and vulnerabilities, when targeted at OPIC-critical assets, can have a serious impact on the ability of OPIC to perform its mission.

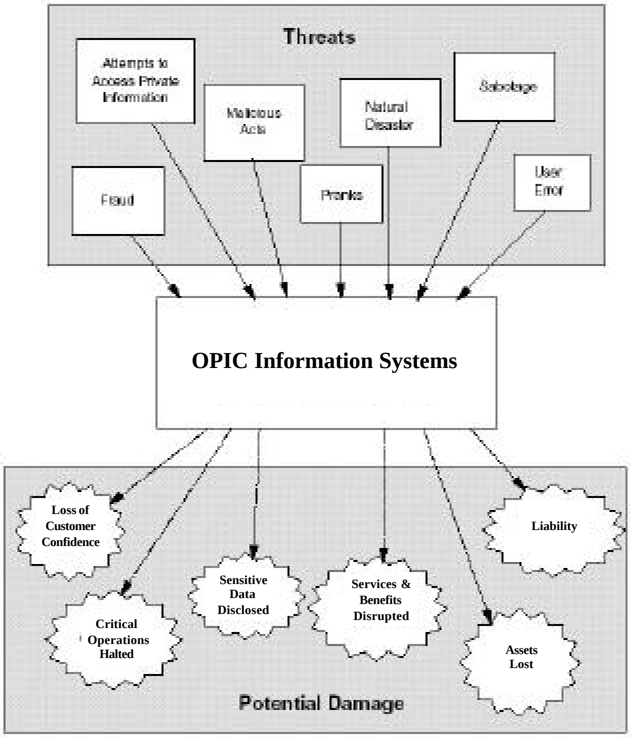


Figure 5-1: Information Security Threats[6]

[6] GAO/AIMD-98-68 Information Security Management, May 1998. P. 8.

5.B.IV.a Errors and Omissions

One of the most common threats to information security is errors and omissions. Everyone at OPIC is at risk of unintentionally making an error that contributes directly or indirectly to security problems. Examples include incorrect data entry, accidental deletion or modification of data, programming mistakes (*i.e.* "bugs"), system administration errors, and inadvertent overloading of the system. These can compromise all three aspects of information security – confidentiality, integrity, and availability.

To combat this threat, it is imperative that OPIC implement the following measures as part of its information security program:

- Information users must receive adequate security awareness training so they can help OPIC reduce the number and severity of errors and omissions.
- Quality control measures must be implemented for information systems, wherever feasible, to guard against these conditions. This includes both technical and procedural validation and verification techniques.
- Standardized procedures should be implemented for IT management and programming functions to reduce potential errors throughout the system lifecycle.
- Procedures for reporting and correcting errors need to be implemented.
- Changes made to systems should be performed in a carefully controlled and documented manner.

5.B.IV.b Fraud and Theft

OPIC's information resources are susceptible to fraud and theft, both from insiders and outsiders. Not only are the resources themselves at risk of being stolen, but they can also be used to commit these acts against other entities and resources. Insiders may try to steal resources (both equipment and data) for personal use, modify data (such as records in the time and attendance systems), use computers to skim money from financial accounts, commit Internet fraud, or misuse these resources in other illegal ways. Outsiders may also steal money, illegally acquire data, or use OPIC's resources to commit fraud. Because insiders are statistically responsible for the majority of computer fraud, and have both access to and familiarity with OPIC systems, they are actually the greater threat to OPIC's information resources.

To guard against fraud and theft, OPIC needs to implement a variety of safeguards, including:

- Set documented rules for what users are and are not allowed to do with OPIC resources (*i.e.* "appropriate use").

- Educate users on OPIC information security policies and the penalties for violating them.
- Ensure that all access to information resources requires identification and authentication of the user, to provide accountability for all system activities.
- Implement audit trails to detect and track fraud and theft.
- Control access to information resources to only those who need access to perform their duties.
- Implement personnel security procedures, such as background screening and separation of duties.
- Deploy perimeter protections to safeguard OPIC resources from external entities who may want to steal them or use them for fraudulent purposes.
- Implement procedures for prompt removal of access rights for terminated personnel.
- Safeguard mobile computing devices.
- Implement procedures for reporting and responding to incidents of fraud and theft.
- Control physical access to critical information resources (such as the computer room).

5.B.IV.c Employee Sabotage

Employee sabotage is less common than fraud or theft, but the cost of such incidents is generally much higher. Common examples of sabotage include deliberate acts of destruction or damage of equipment, deletion or incorrect modification of data, crashing of systems, and distribution of viruses and other malicious programs. Such activities are generally performed by personnel who feel betrayed, cheated, bored, or harassed, particularly those with low job satisfaction or who have been terminated.

Safeguards for the threat of employee sabotage are similar to those for theft and fraud:

- Set documented rules for what users are and are not allowed to do with OPIC resources (*i.e.* “appropriate use”).
- Educate users on OPIC information security policies and the penalties for violating them.
- Ensure that all access to information resources requires identification and authentication of the user, to provide accountability for all system activities.
- Implement audit trails to detect and track employee sabotage.

- Control access to information resources to only those who need access to perform their duties.

- Implement personnel security procedures, such as background screening and separation of duties.

- Control physical access to critical information resources (such as the computer room).

- Implement procedures for prompt removal of access rights for terminated personnel.

- Deploy change control measures to protect systems against unauthorized modification.

- Implement procedures for reporting and responding to incidents of fraud and theft.

5.B.IV.d Loss of Physical and Infrastructure Support

OPIC's facilities are susceptible to disruptions such as utility failures, fires, floods, terrorist acts, and other situations that may affect the availability of critical infrastructure components. These conditions often result in system downtime.

To address this threat, OPIC needs to:

- Perform disaster recovery and continuity of operations planning.

- Implement physical and environmental security measures, such as fire alarms and backup power.

- Build redundancy into critical infrastructure components, such as network and telephony resources.

- Implement procedures for reporting and responding to physical/infrastructure loss incidents.

5.B.IV.e Malicious Hackers

Malicious hackers are people who break into computers without authorization, and may be either outsiders or personnel internal to OPIC. Hackers may have a variety of intentions, including accessing sensitive information, causing damage to systems, theft, modifying data, and causing a denial of service.

To combat hackers, OPIC must address the following security considerations:

- Implement perimeter protections and network security tools to keep unauthorized persons out of the OPIC network.

- Control physical and logical access to OPIC information resources.
- Configure servers according to security standards to minimize risk of being hacked.
- Implement procedures for deploying system updates and security patches in a timely fashion.
- Secure remote access and mobile computing from access by unauthorized persons.
- Utilize encryption and other measures to secure wireless communications.
- Deploy audit trails to track system access.
- Implement procedures for reporting and responding to hacking incidents.

5.B.IV.f Industrial Espionage

"Industrial espionage is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is often referred to as economic espionage."[7]

As with other threats, industrial espionage may be performed by personnel either internal or external to OPIC. Statistically, the most likely sources of this threat are current employees who sell data for profit and disgruntled prior employees who do it for revenge.

Because OPIC has proprietary information from many companies, particularly those doing business internationally, it is a good potential target for industrial espionage. OPIC must take precautions to protect the data that has been entrusted to the agency by its customers. A failure to do so would result in potential liability, damage OPIC's reputation, and possibly affect OPIC's ability to perform its mission in the future.

Steps that can be taken to protect OPIC data from industrial espionage include:

- Perform classification of OPIC data and provide appropriate protections in accordance with the classification level.
- Utilize encryption to secure sensitive information in transmission and in storage.

[7] NIST Special Publication 800-12 "An Introduction to Computer Security: The NIST Handbook", p. 33

- Implement perimeter protections and network security tools to keep unauthorized persons out of the OPIC network.
- Control physical and logical access to specific OPIC information resources.
- Secure remote access and mobile computing from access by unauthorized persons.
- Implement procedures for protection of media containing sensitive data.
- Deploy audit trails to track system access.
- Implement procedures for reporting and responding to industrial espionage incidents.

5.B.IV.g Malicious Code

On of the most prevalent threats to OPIC information resources is malicious code. This includes viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Malicious code may be distributed through email attachments, web scripts, software installations, infected data files, and other methods. These can cause affects ranging from minor annoyance to loss of data or the incapacitation of OPIC systems.

To minimize the effects of malicious code, OPIC needs to:

- Deploy antivirus software that can detect and stop viruses and other malicious code.
- Employ firewalls, email filters and other tools to try to stop such code from entering the OPIC environment.
- Educate users about how to avoid allowing malicious code into OPIC's environment.
- Carefully control the installation of software within OPIC.
- Configure servers and workstations according to security standards to minimize vulnerability to malicious code.
- Implement procedures for deploying system updates and security patches in a timely fashion.
- Implement procedures for reporting and responding to malicious code incidents.

5.B.IV.h Foreign Government Espionage

Because OPIC is a government agency, as well as an entity which has dealings with foreign governments, OPIC could become a target of foreign government intelligence services. "In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files." [8]

Protections against this threat include:

- Perform classification of OPIC data and provide appropriate protections in accordance with the classification level.
- Implement perimeter protections and network security tools to keep unauthorized persons out of the OPIC network.
- Control physical and logical access to OPIC information resources.
- Implement procedures for protection of media containing sensitive data.
- Secure remote access and mobile computing from access by unauthorized persons, especially in international locations.
- Deploy audit trails to track system access.
- Implement procedures for reporting and responding to foreign government espionage incidents.
- Utilize encryption to secure sensitive information in transmission and in storage.

5.B.IV.i Threats to Personal Privacy

OPIC has access to a variety of personal information, such as payroll records and employee background information. This information is susceptible to theft and misuse. In addition to providing protection mandated by the Privacy Act for this information, OPIC has an obligation to protect the information it requests from or creates about employees and other individuals.

[8] NIST Special Publication 800-12 "An Introduction to Computer Security: The NIST Handbook", p. 35

Threats to personal privacy may arise from both insiders and outsiders who wish to sell the information, use it to commit fraud, or simply satisfy curiosity.

In order to protect personal private information, OPIC needs to:

- Perform classification of OPIC data and provide appropriate protections in accordance with the classification level.
- Utilize encryption to secure sensitive information in transmission and in storage.
- Implement perimeter protections and network security tools to keep unauthorized persons out of the OPIC network.
- Control physical and logical access to specific OPIC information resources.
- Secure remote access and mobile computing from access by unauthorized persons.
- Implement procedures for protection of media containing sensitive data.
- Deploy audit trails to track system access.
- Implement procedures for reporting and responding to privacy violation incidents.

6 POLICY FRAMEWORK

Generally speaking, policies are broad statements that summarize management decisions regarding security issues. They provide the basic rules for operating securely within a specific environment. Policies serve to describe what information resources the agency wants to protect. To provide flexibility for use in different systems and situations, policies do not dictate specific technologies or configurations.

Because policies are very high level, OPIC also needs to develop standards, guidelines, and procedures that further define the requirements of the policies and provide guidance on how to implement them.

- *Standards* specify the use of particular technologies, procedures, or configurations in particular situations, and are compulsory. (For example, a standard might be that all Windows 2000 workstations have specific security settings configured in a certain way.)

- *Guidelines* are recommendations that are meant to assist personnel with complying with policy and effectively securing their resources.

- *Procedures* are specific repeatable instructions for completing a particular process (such as the detailed steps for configuring a server or the process for granting access rights to new employees).

6.A Hierarchy

To facilitate their development, administration, and maintenance, OPIC's information security policies have been organized into a logical hierarchy. As OPIC's information security needs evolve, individual policies may be added or removed from this organizational structure. Figure 6-1 illustrates OPIC's information security policy hierarchy. The policies supplement OPIC Management Directive 05-01, *Information Systems Security Program (ISSP),* and are divided into three primary categories:

- *Security Program* – These policies provide guidance for development and operation of the core components of OPIC's information security program, and are derived from FISMA program requirements.

- *Information Resources* – These policies provide guidance on securing specific types of information resources, such as servers, applications, databases, and connectivity components.

- *Security Practices* – These policies provide guidance on implementation and operation of security protections that apply across all OPIC information resources.

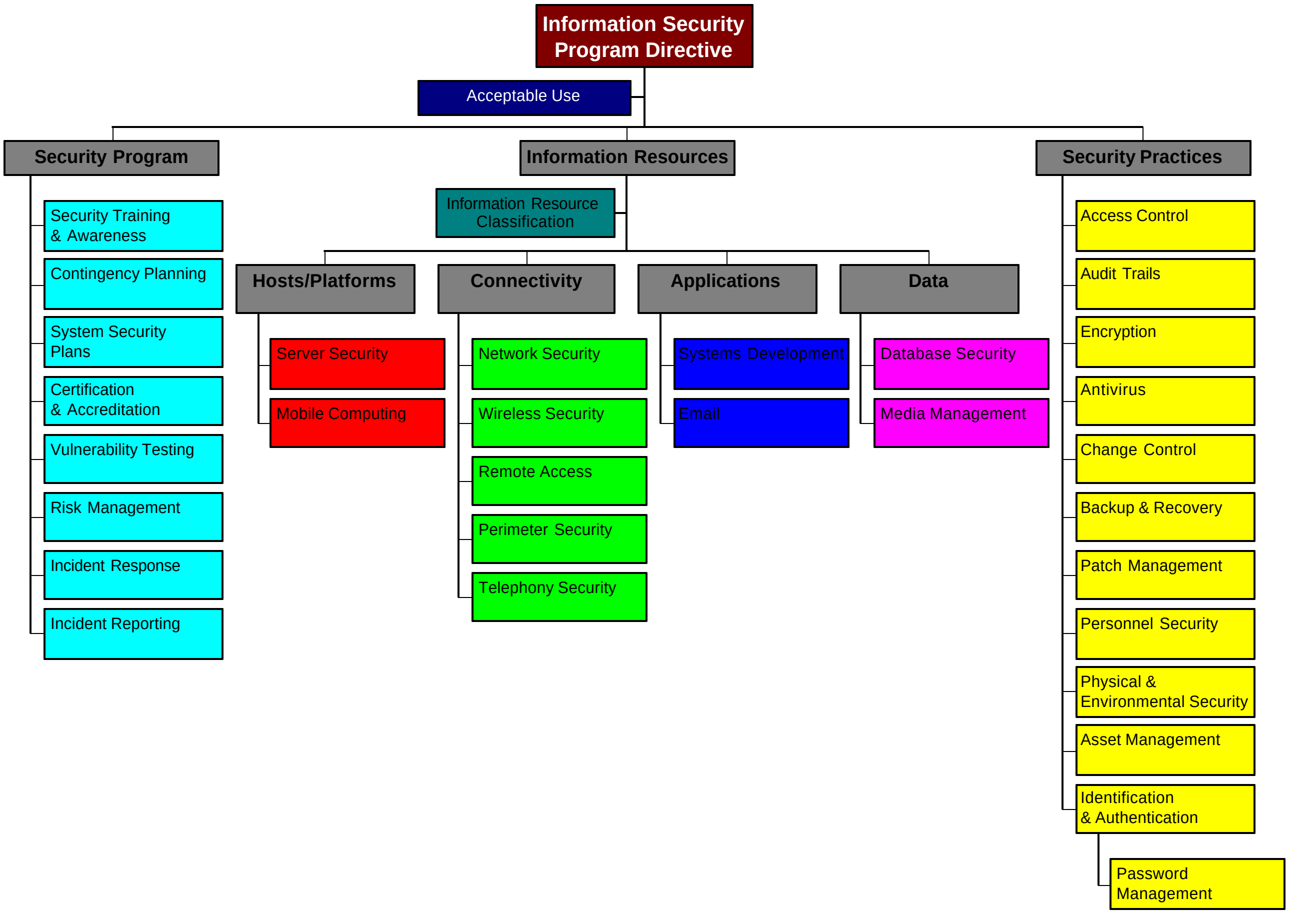


Figure 6-1: OPIC Information Security Policy Hierarchy

6.B Policy Numbering

Each policy is assigned a unique policy number which adheres to the following format:

ISSP-XX-YYMMDD

ISSP designates the policy as part of the Information Systems Security Program.

XX is a unique number assigned to each policy.

YYMMDD is the date that the specific version of the policy was issued.

6.C Policy Structure

Each information security policy is defined as an independent document, and contains all of the information needed to support the policy. The policies are structured to contain the following information:

Policy Name — Formal name of the policy.

Policy Number — Identification number assigned to the policy (see section 6.B).

Subject — Policy statement summarizing the intention of the policy.

Scope — Specification of to whom or what the policy applies.

Description — Explanation of the purpose of the policy.

Procedures, Standards & Guidelines — Narrative stating the specific requirements and directions of the policy. This includes any procedures, standards, and guidelines that must be followed in order to be compliant with the policy.

Roles & Responsibilities — Discussion of responsibilities that apply to each OPIC information security role for complying with the policy. Not all roles will have responsibilities for all policies.

Definitions — Defines key terms used in the policy.

Enforcement — Describes the potential penalties for non-compliance with the policy.

Point Of Contact — Specifies the person to contact for additional guidance or questions about the policy.

Attachments — Lists any associated documents that are incorporated into the policy by reference.

Authority — Enumerates the federal laws, regulations, standards, and other authoritative requirements from which the policy is derived.

Location — Specified the location where the official version of the policy document is stored.

Effective Date — Specifies the date when the policy goes into effect.

Revision History — Lists any revisions that have been made to the policy document.

Review Schedule — Species the frequency with which the policy should be reviewed for potential revision.

6.D Information Security Roles

Everyone at OPIC has a role in maintaining the security of our information resources. For the purpose of assigning security responsibilities, some general roles have been defined. Each policy specifies the particular responsibilities that are assigned to each of these roles as applicable.

Individuals may serve in multiple roles for different aspects of their jobs. For example, a business unit VP may serve as an Information Owner for a particular resource, as a Manager for the employees in his/her department, and as a User of information resources.

The roles specified in the OPIC's information security policies, taken from OPIC Management Directive 05-01, *Information Systems Security Program*, are defined as follows:

- Information Users, as used in these policies, are individuals who use or have access to OPIC's information resources, including employees, interns, temporary workers, contractors, vendors, and visitors.

- Supervisors are employees who have formal supervision of other employees. It is crucial that Supervisors serve as a good example for their employees to follow.

- 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.

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

- The Information Systems Security Officer (ISSO) is the individual designated within OPIC to develop and operate an information security program.

7 POLICIES

Based on the analysis of the information security requirements presented in section 5, OPIC has developed a comprehensive set of policies to meet its security needs. These have been developed in accordance with the framework specified in section 6, and are fully defined in separate, independent documents. The policies include:

Policy Number	Policy Name	Summary
ISSP-01	Acceptable Use Of Information Resources	Individuals using information resources belonging to the Government must act in a legal, responsible, and secure manner, with respect for the rights of others.
ISSP-02	Information Resource Classification	All information resources (including data and systems) must be identified, categorized, and protected in according to their level of sensitivity, criticality, and business “need to know”.
ISSP-03	Risk Management	OPIC must develop, implement, and maintain a risk management program to ensure that appropriate safeguards are employed to protect OPIC resources.
ISSP-04	Security Training & Awareness	OPIC’s information security policies and procedures will be communicated to all employees, and will be made available for reference and review by any other persons in a position to impact the security and integrity of OPIC information resources. A program to maintain awareness of information security policies, standards and acceptable practices will also be implemented.
ISSP-05	Incident Reporting	OPIC personnel and contractors are required to report any suspected security incidents in accordance with OPIC incident reporting procedures.
ISSP-06	Incident Response	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.
ISSP-07	System Security Plans	Each major information system must have an approved security plan.
ISSP-08	Certification And Accreditation	Each major OPIC information system will be certified and accredited every 3 years or upon each significant change to the system (whichever comes first).
ISSP-09	Vulnerability Testing	In order to assess OPIC’s information security posture determine security risks that should be mitigated, OPIC will conduct periodic Vulnerability Assessments. These assessments will assist in the discovery of security vulnerabilities, determine the threat of these vulnerabilities, and assist OPIC in decreasing security risk.
ISSP-10	Contingency Planning	Alternate modes of operation must exist to ensure continuity of critical services in the event of natural disaster, fire, act of terror, or other catastrophic event.
ISSP-11	Access Control	Access to OPIC information resources will be limited to those that need them to perform their duties. The principle of least privilege will be applied to the allocation of access rights.
ISSP-12	Identification And Authentication	Access to OPIC information systems will only be granted to identified and authenticated users.
ISSP-13	Audit Trails	Audit trails must be maintained to provide accountability.
ISSP-14	Antivirus	Standard software and procedures must be implemented to minimize the impact of computer viruses on OPIC’s information resources.

ISSP-15	Encryption	The use of encryption at OPIC will be limited to those algorithms that have been proven to work effectively and which are approved and recommended for government use.
ISSP-16	Personnel Security	Access to OPIC information resources should be limited to only those persons who have been appropriately screened and authorized.
ISSP-17	Physical and Environmental Security	Automated information systems and facilities require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.
ISSP-18	Change Control	All changes made to OPIC information systems will be made in a controlled and coordinated fashion to preserve the confidentiality, integrity, and availability of the system.
ISSP-19	Backup and Recovery	Recoverable backups must be maintained for OPIC information resources.
ISSP-20	Patch Management and System Updates	Systems are to be maintained with updated security patches.
ISSP-21	Server Security	Servers should be made secure before placing them into the OPIC operational environment, and security should be maintained throughout their lifecycle.
ISSP-22	Mobile Computing	Security controls will be implemented to mitigate the increased risks posed by the use of laptops and other mobile devices outside of the OPIC office.
ISSP-23	Network Security	Network devices and connectivity components should be made secure before placing them into the OPIC operational information technology environment, and security should be maintained throughout their lifecycle.
ISSP-24	Perimeter Security	Access to OPICNET will be protected from external threats.
ISSP-25	Remote Access	Security controls will be implemented to mitigate the increased risks posed by allowing remote connectivity into OPICNET.
ISSP-26	Telephony Security	OPIC's telephony resources will be protected against threats to their confidentiality, availability and integrity.
ISSP-27	Wireless Security	When using wireless networks or handheld devices, OPIC should assess the risks involved with that technology, to take steps to reduce those risks to an acceptable level, and to ensure that the level of protection is maintained.
ISSP-28	Systems Development	Security will be integrated into the systems development lifecycle in order to ensure the efficient and effective implementation of appropriate safeguards.
ISSP-29	Electronic Mail	Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.
ISSP-30	Database Security	Information must remain consistent, complete, and accurate.
ISSP-31	Media Management	Media must be handled, stored, and disposed of properly in order to protect the sensitive or critical OPIC data stored upon it.
ISSP-32	Password Management	OPIC will protect access to its information resources by ensuring that any passwords used for authentication are properly assigned and protected.
ISSP-33	Asset Management	All information assets must be tracked and managed to ensure that they are not lost or misused.

8 APPENDIX A: FEDERAL REQUIREMENTS

8.A Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

FISMA's goal is to improve the security of Federal information and information systems. FISMA was enacted into law as Title III of the E-Government Act of 2002 (P.L. 107-347, December 17, 2002). FISMA, along with OMB policy (see Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting (M-03-19) August 6, 2003), lays out a framework for annual IT security reviews, reporting, and remediation planning. Under this framework, the Federal government is able to quantitatively determine both IT security progress and problems. This information is essential to ensuring that remediation efforts and IT resources are prioritized, resulting in the timely resolution of IT security weaknesses.

FISMA requires the head of each agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification or destruction of its information and information systems. FISMA requires Federal agencies to provide risk-based information security protections for information collected as well as information systems used, operated or maintained by or on behalf of an agency. To provide this protection, FISMA requires agencies to establish risk-based information security programs that include periodic risk assessments, use of controls and techniques to comply with information security standards, training requirements, periodic testing and evaluation, reporting, and plans for remedial action, security incident response, and continuity of operations. FISMA requires annual independent evaluation of Federal agency information security programs and practices to determine their effectiveness, and requires each Federal agency to report to Congress annually (via OMB) by the first of March. The report must address the adequacy and effectiveness of information security policies, procedures and practices.

Under FISMA, agency information security activities, other than for classified and other national security systems, are guided by OMB policy and the development of information security standards by NIST that are to include minimum mandatory requirements by risk level. OMB (Office of E-Government) and agency responsibilities are detailed in section 301. Standards are addressed in sections 302 and 303.

FISMA requires the agency head to:

- ❖ Ensure the agency has a sufficient number of trained personnel to ensure agency-wide IA.
- ❖ Require annual reports from the CIO regarding the effectiveness of agency IA programs and progress on any required remedial actions.

FISMA requires the agency CIO to carry out the following responsibilities:

- Develop and maintain an agency-wide information assurance (IA) program complete with policies, procedures and control techniques to address information security requirements, including FISMA.
- Ensure that required training is conducted including annual information security training and Internet security training.
- Designate a senior official responsible of agency information security and ensure oversight of personnel with significant responsibilities for information security.
- Assist senior agency officials concerning their awareness and responsibilities for information and information system security.

Specifically, FISMA requires each Federal agency to develop, document and implement an agency-wide information security program, which includes the following:

- Periodic risk assessments.
- Risk assessment policies and procedures that cost-effectively reduce the risk to an acceptable level, ensure that information security is addressed throughout the life cycle of each agency information system and ensure compliance with FISMA.
- Subordinate plans for networks, facilities and groups of systems as appropriate.
- Security awareness training for agency personnel, including contractors and system users.
- Annual independent evaluation of the agency information security program to determine the effectiveness of such program and practices (which must include periodic but at least annual testing and evaluation of the effectiveness of information security policies, procedures and practices).
- Processes for planning, implementing, evaluating and documenting remedial action to address deficiencies in agency information security policies, procedures and practices.
- Procedures for detecting, reporting and responding to security incidents.
- Plans and procedures to ensure continuity of operations for information systems that support agency operations and assets.

Relationship to other laws/directives: FISMA was enacted with the intention of superseding earlier very similar FISMA provisions enacted into law in the Homeland Security Act (P.L. 107-

296,Title X, November 25, 2002). FISMA replaces GISRA, the Government Information Security Reform provisions of the FY 2001 National Defense Authorization Act (P. L. 106-398, sec. 1061-1064), which was in effect from November 2000 through November 2002 and required Federal agencies to establish agency-wide risk-based information systems security programs and undergo annual independent evaluations. FISMA replaced GISRA with stronger permanent provisions, including requirements for minimum mandatory information systems security standards.

FISMA also supercedes or repeals provisions of the Computer Security Act of 1987 (P.L. 100-235). The CSA directed NIST to develop information technology standards and directed agencies to identify and develop security plans for computer systems containing sensitive but unclassified information. FISMA strengthened NIST's development of standards, particularly information systems security standards, and subsumed the CSA's system requirements within its information systems security program requirements.

8.B OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, November 28, 2000.

OMB Circular A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, (P.L. 104-13 and 44 U.S.C. Chapter 35, which established "a broad mandate for agencies to perform their information resources management activities in an efficient, effective, and economical manner"). Appendix III contains guidance on the "Security of Federal Automated Information Systems." The Appendix establishes a minimum set of controls to be included in Federal automated information security programs, assigns Federal agency responsibilities for the security of automated information, and links agency automated information security programs and agency management control systems established in accordance with OMB Circular A-123.

Appendix III defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act.

Appendix III requires agencies, at a minimum, to include the following controls in their general support systems and major applications:

- ❖ Assign responsibility for security.
- ❖ Develop System Security Plan, a summary of which must be incorporated into the strategic IRM plan, and which must include rules of the system, training, personnel

controls, incident response cabability, continuity of support, technical security, and system interconnection.

- Develop Application Security Plan which must include application rules, specialized training, personnel security, contingency planning, technical controls, information sharing, and public access controls.
- Review security controls whenever significant modifications are made to the application/system and at least every three years.
- Re-authorize use of the system at least every three years.

The Appendix requires agencies to provide two reports to OMB:

1. Agencies are required to correct deficiencies identified through the reviews of security for systems and major applications and, if a deficiency in controls is judged by the agency head to be material when weighed against other agency deficiencies, to include it in the annual FMFIA report. Less significant deficiencies must be reported and progress on corrective actions tracked at the appropriate agency level.
2. Agencies are also required to include a summary of their system security plans and major application plans in their agency strategic information resources management plans required by the Paperwork Reduction Act (44 U.S.C. 3506).

Finally, Appendix III also defines responsibilities of various agencies, including the Department of Commerce, Department of Defense, Department of Justice, the General Services Administration, The Office of Personnel Management, and the Security Policy Board.

Relationship to other laws/directives: The Appendix incorporates requirements of the Computer Security Act of 1987 (P.L. 100-235) and responsibilities assigned in applicable national security directives.

8.C Homeland Security Presidential Directive / HSPD-7, December 17, 2003.

HSPD-7 established a national policy for Federal agencies for security protection and requires agency heads to identify, prioritize, assess, remediate, and protect their respective internal critical infrastructure and key resources in order to prevent, deter, and mitigate the effects of deliberate efforts to destroy, incapacitate, or exploit those resources. Consistent with the Federal Information Security Management Act of 2002, agencies must identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

The Directive requires that by July 2004, the heads of all Federal agencies develop and submit to the Director of OMB for approval plans for protecting the physical and cyber critical infrastructure and key resources that they own or operate. These plans must address identification, prioritization, protection, and contingency planning, including the recovery and reconstitution of essential capabilities.

Relationship to other laws/directives: HSPD-7 supersedes Presidential Decision Directive 63, May 22, 1998, Subject: Critical Infrastructure Protection.

8.D OMB Memo M-04-04, E-Authentication Guidance for Federal Agencies, December 16, 2003.

OMB Memo M-04-04 updates guidance issued by OMB under the Government Paperwork Elimination Act of 1998 (44 U.S.C. § 3504), and implements section 203 of the E-government Act (44 U.S.C. ch. 36). While not all Federal electronic transactions require authentication, the guidance applies to all such transactions for which authentication is required, regardless of the constituency (*e.g.*, individual user, business, or government entity).

The guidance takes into account current practices in the area of authentication (or e-authentication) for access to certain electronic transactions, as well as the need for government-wide standards, and assists agencies in determining their authentication needs for electronic transactions. The guidance directs agencies to conduct "e-authentication risk assessments" on electronic transactions to ensure that there is a consistent approach across government. It also provides the public with clearly understood criteria for access to Federal government services online.

Agencies must categorize all existing transactions/systems requiring user authentication into one of several described assurance levels by September 15, 2005, and should do so in the following order:

- Systems classified as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design, within 90 days of the completion of the final E-Authentication Technical Guidance issued by the National Institute of Standards and Technology (NIST).

The chosen assurance level must be made publicly available through the agency website, the Federal Register, or other means (*e.g.*, upon request). Agency application assurance levels will be posted at a central location for public access by the E-Authentication Initiative.

Beginning in 2004, agencies will be asked to report on their progress in implementing this guidance in their annual E-Government Act Reports to OMB required by section 202(g) of the E-Government Act.

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

OMB Memo M-99-20 reminds agencies that, consistent with the principles embodied in OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources", they must continually assess the risk to their computer systems and maintain adequate security commensurate with that risk.

The guidance required agencies to conduct within 90 days a review of security practices to ensure that they had in place a process that permits program officials and security managers to understand the risk to agency systems and take necessary steps to mitigate those risks. This process must include specific procedures to ensure the timely implementation of security patches for known vulnerabilities, especially for those systems that are accessible via the Internet.

The guidance notified agencies of NIST's Computer Security Resources Clearinghouse website (http://csrc.nist.gov) and NIST's Information Technology Laboratory (ITL), which produces a periodic bulletin that provides up-to- date information on significant security issues. The guidance also notified agencies of the Federal Incident Response Capability (FedCIRC), which issues security advisories and offers free baseline services such as incident response and other, fee-based services such as on-site recovery and audit trail analysis.

8.F The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.

Broadly stated, the Privacy Act seeks to balance the government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them. The Act focuses on four basic policy objectives:

(1) To restrict disclosure of personally identifiable records maintained by agencies.

(2) To grant individuals increased rights of access to agency records maintained on themselves.

(3) To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete.

(4) To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The Act defines a "system of records" as any group of records under the control of a Federal agency or agent thereof from which information is retrieved by the name of the individual or by some identifying number, symbol, or their identifying particular (*e.g.*, fingerprint). The retrieval does not have to pinpoint a particular John Doe, but rather any John Doe, so this implies that Privacy Act protections apply to virtually any database that collects information on people along with their name (and/or SSN, and/or phone number, etc.), as long as that data is collected on behalf of a Federal agency.

The Act defines twelve specific conditions for disclosure of collected information; requires accurate accounting (audit) of disclosures, changes to data, etc.; defines rules for access to data, most of which focuses of rights of individuals to access/correct their data; requires agencies to inform each individual who is asked to submit data of routine use, etc.; and requires agencies maintaining systems of records to publish in Federal Register: categories of individuals, records, and sources of records, each routine use of records, and procedures for individual to be notified.

The Act requires agencies to establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and to instruct each person on the rules and the requirements of the Privacy Act. The Act also requires agencies to establish appropriate administrative, technical and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

8.G Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

PDD 67 recognizes emerging threats, addresses enduring constitutional government, and introduces continuity of operations planning (COOP) and continuity of government operations. PDD 67, among other things, requires Federal agencies to develop COOP plans for essential operations. These COOP plans are viewed as a unifying concept not to replace existing plans but, instead, to be superimposed if and when a problem threatens a serious disruption of agency operations. PDD 67 designates FEMA as the Executive Agent for COOP.

PDD 67 required that viable COOP capability must be achieved by Oct. 21, 1999. It takes an all hazards approach, requires agencies to address the use of alternate facilities, requires that agencies be able to operate within 12 hours of activation of COOP, and requires agencies to be able to sustain COOP operations for up to 30 days.

Several Federal Preparedness Circulars (FPCs) that detail a series of government policies specific to COOP planning and national security emergency preparedness have been written under the authority of PDD 67. The focus of these documents includes succession, vital records, training, COOP requirements, alternative facility requirements, and communications. They are associated with supporting all Federal organizations with viable COOP programs. FPC 65 provides guidance to all Federal Executive Branch departments, agencies, and independent organizations on the development of viable and executable COOP plans. FPC 66 further supports COOP efforts by providing guidance on the development of test, training, and exercise programs to support the implementation and validation of COOP plans. FPC 67, designed as a supplement to FPC 65, provides guidance on implementing COOP plans, specifically in locating alternate facilities to support COOP efforts.

Relationship to other laws/directives: PDD 67 succeeded NSD 69 "Enduring Constitutional Government" of June 1992.

8.H Clinger-Cohen Act of 1996, PL 104-106, February 10, 1996.

The Clinger-Cohen Act encourages performance-based and results-based management through the effective use of information technology (IT). It shifts the emphasis from IT acquisition management to IT investment management, and emphasizes information resources management and IT management (not information management). The Act requires the heads of Federal agencies to link IT investments to agency accomplishments. It also requires that agency heads establish a process to select, manage and control their IT investments.

The Clinger-Cohen Act repeals the Brooks Act and returns IT procurement authority to Federal agencies. It transfers day-to-day management of IT from GSA to OMB, with the exception of FTS2000. The effect is to eliminate the Federal Information Resources Management Regulations (GSA has moved some provisions to the Federal Acquisition Regulations) and the General Services Board of Contract Appeals. The law gives OMB responsibility for:

- Developing a process for analyzing, tracking, and evaluating the risks and results of major capital investments,
- Directing executive agencies on establishing an effective, efficient IT capital planning and investment review process, and
- Enforcing accountability through the budget process.

The law gives executive agencies responsibility for:

- Establishing an IT capital planning and investment review process,
- Using performance measures to assess how well IT supports programs, and
- Justifying continuation of systems that deviate from cost, performance, or schedule goals.

The Clinger-Cohen Act establishes a Chief Information Officer (CIO) in executive agencies who:

- Reports directly to the agency head,
- Has IRM as the primary duty,
- Provides advice and assistance to the agency head on IT and information resources management,
- Develops an integrated IT architecture,

- Promotes efficient and effective design and operation of IRM processes,
- Uses performance measures to monitor IT programs,
- Assesses the knowledge and skills of IRM personnel,
- Shares with the CFO responsibility for provision of financial and performance data for financial statements, and
- Assumes the responsibilities of the Designated Senior Official defined in Paperwork Reduction Act.

Clinger-Cohen confirms the responsibility of NIST for standards and guidelines for computer systems and reinforces requirements of the Computer Security Act. It also encourages and provides for modular contracting for IT systems and pilot IT acquisition programs.

Relationship to other laws/regulations: The Clinger-Cohen Act of 1996 renames the Information Technology Management Reform Act and the Federal Acquisition Reform Act.

8.I Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994 [18 USC, Chapter 47, Section 1030].

The Computer Abuse Amendments Act of 1994 expanded the Computer Fraud and Abuse Act of 1986 to address the transmission of viruses and other harmful code. Codified at 18 USC, Chapter 47, Section 1030, it prohibits unauthorized or fraudulent access to government computers, and establishes penalties for such access.

The Act makes six types of activity illegal:

1. Acquiring national defense, foreign relations, or restricted atomic energy information with the intent or reason to believe that the information can be used to injure the United States or to the advantage of any foreign nation. (The offense must be committed knowingly by accessing a computer without authorization or exceeding authorized access.)
2. Obtaining information in a financial record of a financial institution or a card issuer, or information on a consumer in a file of a consumer reporting agency. (The offense must be committed intentionally by accessing a computer without authorization or exceeding authorized access.)
3. Affecting a computer exclusively for the use of a U.S. government department or agency or, if it is not exclusive, one used for the government where the offense adversely affects the use of the government's operation of the computer. (The offense must be committed intentionally by accessing a computer without authorization.)

4. Furthering a fraud by accessing a federal interest computer and obtaining anything of value, unless the fraud and the thing obtained consists only of the use of the computer. (The offense must be committed knowingly, with intent to defraud, and without authorization or exceeding authorization.)

5. Through use of a computer used in interstate commerce, knowingly causing the transmission of a program, information, code, or command to a computer system.

6. Furthering a fraud by trafficking in passwords or similar information which will allow a computer to be accessed without authorization, if the trafficking affects interstate or foreign commerce or if the computer affected is used by or for the government. (The offense must be committed knowingly and with intent to defraud.)

Under the Amendments, prosecutors no longer have to prove "harmful intent," but a less strict "reckless disregard" standard, to convict. The Amendments also broaden the scope of the protection offered in section 1030 (a) (5) (A) in order to close a loophole contained in the earlier Act. "[I]ntentionally accesses a Federal interest computer" is no longer used, and instead the section applies to anyone who "through means of a computer used in interstate commerce or communications, knowingly causes the transmission of a program, information, code, or command to a computer or computer system ...." As amended, the section now protects not only Federal interest computers, but it also covers privately owned computer systems, used in interstate commerce or communication, but which may be affected by someone acting through means of a computer located within the same state as the affected computer.

The Amendments also remove the "access" requirement from the statute. Instead, a specific intent to perform certain acts that may constitute direct or indirect access is put into the statute. Significantly, the statute also adds a requirement that there be either a specific intent or reckless disregard as to whether the transmission will cause damage or withhold or deny use of a "computer, computer system, network, information, data, or program" in excess of the user's authorization.

8.J Computer Security Act of 1987, PL 100-235, January 8, 1988.

The Computer Security Act of 1987 was enacted to mandate that federal agencies take extra measures to prevent unauthorized access to computers holding sensitive information. It requires each agency to establish a plan for the security and privacy of sensitive information, and requires the submission of such plans to NIST and the National Security Agency for advice and comment. These plans are subject to disapproval by the Office of Management and Budget.

The Act requires Federal agencies to provide for mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a Federal computer system within or under the supervision of the Federal agency. This includes contractors as well as employees of the agency.

The Act directs NIST to establish a computer standards program for Federal computer systems, including guidelines for the security of such systems. It sets forth authorities of NIST in implementing such standards, and requires NIST to draw upon computer system technical security guidelines developed by the National Security Agency regarding protecting sensitive information.

The Computer Security Act also charged NIST, together with the U.S. Office of Personnel Management (OPM), with developing and issuing guidelines for Federal computer security training. This requirement was satisfied by NIST's issuance of *Computer Security Training Guidelines* (Special Publication [SP] 500- 172), in November 1989. In January 1992, OPM issued a revision to the Federal personnel regulations, which made these voluntary guidelines mandatory. This regulation, *Employees Responsible for the Management or Use of Federal Computer Systems*, requires Federal agencies to provide training as set forth in the NIST guidelines.

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

The Computer Fraud and Abuse Act of 1986 was initially aimed at protecting “federal interest” computers as well as computers used by financial institutions but now protects any computer used in interstate commerce. Specifically, the law prohibits the use of "a program, information, code or command" with intent to damage, cause damage to, or deny access to a computer system or network. In addition, the Act specifically prohibits even unintentional damage if the perpetrator demonstrates reckless disregard of the risks of causing such damage.

The Act imposes penalties on individuals who knowingly and with intent to defraud gain unauthorized access to computers. Although the Act does not include provisions for critical information infrastructure protection per se, it has played a major role in prohibiting and sanctioning cyber attacks. Congress has continued to amend the law over the last several years to increase its effectiveness as the threat and technology have evolved.

Relationship to other laws/directives: Amended by the Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994.

8.L 1991 U.S. Federal Sentencing Guidelines

The 1991 U.S. Federal Sentencing Guidelines provide punishment guidelines for those found guilty of breaking federal law. Certain of these guidelines are pertinent to information security:

- Treat the unauthorized possession of information without the intent to profit from the information as a crime.
- Address both individuals and organizations.

- Make the degree of punishment a function of the extent to which the organization has demonstrated "Due diligence"(*due care*) in establishing a prevention and detection program.

- Invoke the "prudent man rule" that requires senior officials to perform their duties with the care that ordinary, prudent people would exercise under similar circumstances.

- Place responsibility on senior organizational management for the prevention and detection programs.

8.M NIST Guidance

Founded in 1901, NIST is a non-regulatory federal agency within the U.S. Commerce Department's Technology Administration. NIST's mission is to develop and promote measurement, standards, and technology to enhance productivity, facilitate trade, and improve the quality of life.

Under the Computer Security Act of 1987, NIST's Computer Security Division develops security standards and guidelines for sensitive (unclassified) Federal IT systems and works with industry to help improve the security of commercial IT products. The Division has key focused activities in the areas of cryptographic standards and applications, security of emerging technologies, security management, and security testing. The mission of NIST's Computer Security Division is to improve information systems security by:

- Raising awareness of IT risks, vulnerabilities and protection requirements, particularly for new and emerging technologies;

- Researching, studying, and advising agencies of IT vulnerabilities and devising techniques for the cost-effective security and privacy of sensitive Federal systems;

- Developing standards, metrics, tests and validation programs:

    - to promote, measure, and validate security in systems and services

    - to educate consumers and

    - to establish minimum security requirements for Federal systems

- Developing guidance to increase secure IT planning, implementation, management and operation.

FISMA reaffirmed and strengthened NIST's role as the developer of information security standards for use throughout the federal government.

NIST's publications present the results of NIST studies, investigations, and research on information technology security issues. The publications are issued as Special Publications (Spec. Pubs.), NISTIRs (Internal Reports), and ITL (formerly CSL) Bulletins. Special Publications series include the Spec. Pub. 500 series (Information Technology) and the Spec. Pub. 800 series (Computer Security). Computer security-related Federal Information Processing Standards (FIPS) are also included. As a federal agency, OPIC must adhere to these information security standards and guidelines whenever possible.

9 APPENDIX B: ACRONYMS AND ABBREVIATIONS

AV	AntiVirus
C&A	Certification and Accreditation
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CM	Configuration Management
COOP	Continuity of Operations Plan
CSA	Computer Security Act
DAA	Designated Approving Authority
EO	Executive Order
FEDCIRC	Federal Computer Incidental Response Center
FISMA	Federal Information Security Management Act
FMFIA	Federal Managers Financial Integrity Act
FOIA	Freedom of Information Act
FPC	Federal Preparedness Circular
GAO	Government Accounting Office
GISRA	Government Information Security Reform Act
GSA	General Services Administration
HSPD	Homeland Security Presidential Directive
InfoSec	Information Security

IRM	Information Resources Management
ISC^2	International Information Systems Security Certifications Consortium
ISSO	Information Systems Security Officer
ISSP	Information Systems Security Program
IT	Information technology
ITL	Information technology Laboratory
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PC	Personal Computer
PDD	Presidential Decision Directive
PL	Public Law
POC	Point of Contact
SDLC	Systems Development Lifecycle
SETA	Security Education, Training & Awareness
SP	Special Publication
SSN	Social Security Number
ST&E	Security Test and Evaluation
USC	United States Code

ACCEPTABLE USE OF INFORMATION RESOURCES

ISSP-01-0410

1. **SUBJECT:** Individuals using information resources belonging to the Federal government must act in a legal, ethical, responsible, and secure manner, with respect for the rights of others.

2. **SCOPE:** This policy applies to all users of OPIC information resources.

3. **DESCRIPTION:** Inappropriate use of information resources exposes OPIC to risks including compromise of systems and services, legal issues, financial loss, and damage to reputation. The purpose of this policy is not to impose restrictions that are contrary to OPIC's established culture of openness, trust and integrity, but to protect OPIC's employees and the government from illegal or damaging actions by individuals, either knowingly or unknowingly.

   Access to computers, computing systems and networks owned by the government is a privilege which imposes certain responsibilities and obligations, and which is granted subject to OPIC policies and guidelines, and governing laws. This policy sets forth the principles that govern appropriate use of information resources, and is intended to promote the efficient, ethical and lawful use of these resources. Individuals using information resources belonging to the government must act in a responsible manner, and with respect for the rights of others.

4. **PROCEDURES & GUIDELINES:**

   (a) Employees shall use OPIC-provided information resources for OPIC-related business in accordance with their job functions and responsibilities, except as otherwise provided by management directives or other OPIC policies.

   (b) As set forth in OPIC Directive 94-04, employees are permitted limited personal use of information resources if the use does not result in a loss of employee productivity, interfere with official duties or business, and involves minimal additional expense to the government. Unauthorized or improper use of information resources may result in loss of use or limitations on use of those resources.

   (c) When using government information resources, employees are expected to:

      (1) Act responsibly so as to ensure the ethical use of OPIC information resources in compliance with the Standards of Ethical Conduct for Federal Employees.

      (2) Acknowledge the right of OPIC to restrict or rescind computing privileges at any time.

      (3) Use security measures to protect the confidentiality, integrity, and availability of information, data, and systems.

      (4) Conduct themselves professionally in the workplace and to refrain from using government information resources for activities that are inappropriate.

(5) Respect all pertinent licenses, copyrights, contracts, and other restricted or proprietary information.

(6) Use good judgment in accessing the Internet. Each use of the Internet should be able to withstand public scrutiny without embarrassment to OPIC or the federal government.

(7) Safeguard their user IDs and passwords, and use them only as authorized. Any actions taken under an assigned identification (*e.g.*, userid) are the responsibility of the user.

(8) Respect government property.

(9) Make only appropriate use of data to which they have access.

(10) Exercise good judgment regarding the reasonableness of personal use.

(11) Use information resources efficiently.

(d) The following activities are strictly prohibited:

(1) Intentionally corrupting, misusing, or stealing software or any other computing resource.

(2) Accessing OPIC systems that are not necessary for the performance of the employee's duties.

(3) Performing functions that are not related to the employee's job responsibilities on systems that they are otherwise authorized to access.

(4) Making unauthorized changes to OPIC computer resources, including installation of unapproved software or interfering with security measures (such as audit trail logs and antivirus software).

(5) Copying OPIC proprietary software or business data for personal or other non-government use.

(6) Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which OPIC or the end user does not have an active license.

(7) Disseminating trade secrets or business sensitive information, except as permitted by law or regulation.

(8) Transmitting, storing, or processing classified data except as authorized and in accordance with OPIC Directive 94-14, *OPIC Security Program*.

(9) Unauthorized access to other computer systems using OPIC information resources.

(10) Accessing information resources, data, equipment, or facilities in violation of any restriction on use.

(11) Using government computing resources for personal or private financial gain.

(12) Using another person's computer account, with or without their permission.

(13) Implementing any computer systems without authorization from IRM.

(14) Knowingly, without written authorization, executing a program that may hamper normal OPIC computing activities.

(15) Adding components or devices (e.g., PDAs, thumb drives, cameras, etc) to OPIC desktops without explicit approval from the Director of Technical Services.

(16) Introducing malicious programs into the network or server (*e.g.*, viruses, worms, Trojan horses, e-mail bombs, etc.).

(17) Revealing account passwords to others or allowing the use of one's account by others, including family and other household members when work is being done at home.

(18) Revealing system passwords (e.g. FPPS passwords, database passwords, etc) to anyone who is not specifically authorized to use them.

(19) Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws.

(20) Effecting security breaches or disruptions of network communication.

(21) Unauthorized security scanning, network monitoring, or data interception that is not part of the employee's regular job duties.

(22) Circumventing any OPIC information security measures.

(23) Interfering with or denying service to other information resource users.

(24) Providing information about, or lists of, OPIC employees to parties outside of the government that are not required for OPIC business.

(25) Sending unsolicited email messages (spam).

(26) Any form of harassment via email, telephone, pager, IRC, SMS, or other communication method, whether through language, frequency, or size of messages.

(27) Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.

(28) Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity without specific permission from OPIC.

(29) Posting agency information to external news groups, bulletin boards or other public forums without authority, or conducting any activity that could create the perception that communication was made in one's official capacity as a Federal government employee, unless appropriate Agency approval has been obtained.

(30) Any personal use that could cause congestion, delay, or disruption of service to any government system or equipment.

(31) Using government office equipment or information resources for activities that are illegal, inappropriate, or offensive to fellow employees or the public. This includes, but is not limited to, materials related to:

- Sexually explicit or sexually oriented content
- Ethnic, racial, sexist, or other offensive comments
- Anything that is in violation of sexual harassment or hostile workplace laws
- Making fraudulent offers of products, items, or services.
- Gambling
- Illegal weapons or terrorist activities
- Planning or commission of any crime

(32) Forging or misrepresenting one's identity.

(e) Auditing and Privacy:

(1) All use of OPIC information resources may be monitored by OPIC.

(2) Employees do not have an expectation of privacy or anonymity while using any government information resource at any time, including accessing the Internet and email.

(3) Users agree to be governed by acceptable usage policies and to have their usage audited. By using government office equipment, employees imply their consent to disclosing the contents of any files or information maintained or passed-through government office equipment.

(4) To the extent that employees wish that their private activities remain private, they should avoid using agency office equipment such as their computer, the Internet, or E-mail, for those activities.

(5) Auditing procedures will be implemented to ensure compliance with OPIC security policies.

(6) System administrators have the ability to audit network logs, employ monitoring tools, and perform periodic checks for misuse.

(f) Employees agree to be bound by the following conditions for continued use of OPIC information resources:

(1) Employees and contractors will sign an agreement to comply with OPIC information security policy.

(2) Personnel with administrative access or elevated privileges to any IT resources will sign an Elevated Privileges Usage Agreement.

(g) Usage of OPIC IT resources for illegal purposes will be reported to appropriate authorities.

5. ROLES & RESPONSIBILITIES:

(a) Information Users are responsible for:

(1) Using information resources responsibly and in compliance with all OPIC information security policies and guidelines.

(2) Reporting any suspected inappropriate use of information resources to either their manager or the ISSO.

(b) Supervisors are responsible for:

(1) Ensuring that their personnel understand OPIC policy regarding acceptable usage of information resources.

(2) Monitor their employees' use of information resources.

(c) Information Owners are responsible for implementing measures to protect their resources against inappropriate use.

(d) Information Custodians are responsible for assisting information owners with implementing measures to protect their resources against inappropriate use.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing usage of the OPIC information resources to ensure compliance with policies and guidelines.

6. DEFINITIONS:

(a) Access - The right to enter or make use of a computer system. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

(b) Administrative Access – Enhanced privilege level that allows the user to perform administration of the system.

(c) Account - A set of privileges for authorization to system access, which are associated with a userid.

(d) Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

(e) Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

(f) Information Custodians - Individuals (*e.g.*, IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner's requirements for processing, telecommunications, protection controls, and output distribution for the resource.

(g) Information Owners - 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.

(h) Information Users - Individuals who use or have access to OPIC's information resources, including employees, vendors, and visitors.

(i) Password - Any secret string of characters which serves as authentication of a person's identity (personal password), or which may be used to grant or deny access to private or shared data (access password).

(j) Personal Use - Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

(k) System Administrator - A designated individual who has special privileges to maintain the operation of a computer application or system.

7. **ENFORCEMENT:** Unauthorized or improper use of government information resources could result in loss or limitations of use of these 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) OPIC Directive 98-02, Use of the Internet and Electronic Mail

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

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

(e) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(f) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(g) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(h) 5 C.F.R. Part 735, Employee Responsibilities and Conduct

(i) 5 C.F.R. Part 2635, Standards of Ethical Conduct for Employees of the Executive Branch

(j) Part 1 of Executive Order 12674, Implementing Standards of Ethical Conduct for Employees of the Executive Branch

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

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

INFORMATION RESOURCE CLASSIFICATION

ISSP-02-0410

1. **SUBJECT:** All information resources (including data and systems) must be identified, categorized, and protected according to their level of sensitivity, criticality, and business "need to know."

2. **SCOPE:** This policy applies to all OPIC information systems and data created, owned, stored, or transferred by OPIC that are not designated as national security classified.

3. **DESCRIPTION:** In order to ensure that appropriate levels of protection are applied to information resources, a framework is needed to classify those resources based on their criticality to the organization and the sensitivity of the data that they contain. This includes developing procedures and standards for assessing the criticality and sensitivity of the systems, and determining minimum security requirements based on those classification levels.

4. **PROCEDURES & GUIDELINES:**

   (a) All OPIC information resources will be categorized based on OPIC's information classification framework.

   (b) Risks and threats to information resources will be assessed, and security measures will be applied, based on the resource's classification level, in accordance with OPIC risk management procedures.

   (c) OPIC's information classification framework will be based on NIST guidance, as presented in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, and Special Publication 800-60, Guide For Mapping Types of Information and Information Systems to Security Categories, as well as subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for:

      (1) Categorizing their resources in accordance with OPIC's classification framework.

      (2) Ensuring that their resources are protected commensurate with their categorization level.

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

      (1) Developing and communicating OPIC's information classification framework.

      (2) Assisting information owners with assessing the classification level of their resources.

      (3) Auditing to ensure compliance with this policy.

6. **DEFINITIONS:**

(a) Information Resources – The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

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) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(f) Computer Security Act of 1987, PL 100-235, January 8, 1988.

(g) Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

(h) FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems

(i) NIST Special Publication 800-60, Guide For Mapping Types of Information and Information Systems to Security Categories.

(j) 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.

RISK MANAGEMENT

ISSP-03-0410

1. **SUBJECT:** OPIC must develop, implement, and maintain a risk management program to ensure that appropriate safeguards are employed to protect OPIC resources.

2. **SCOPE:** This policy applies to all OPIC information resources.

3. **DESCRIPTION:** In determining a security strategy for a system or the organization, OPIC must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business, while addressing financial and operational concerns. The objective of performing risk management is to enable OPIC to accomplish its mission by:

   ❖ Better securing the IT systems that store, process, or transmit organizational information.

   ❖ Enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget.

   ❖ Assisting management in authorizing (or accrediting) their IT systems on the basis of the supporting documentation resulting from the performance of risk management.

   Risk management is an essential management function and should not be treated solely as a technical function relegated to IT operational or security personnel for implementation. Effective risk management processes support sound *risk-based decision-making.* The CIO and other OPIC executives need to ensure implementation of an effective and comprehensive risk management program, which encompasses all segments of the enterprise, in order to support OPIC's mission.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will use a risk-based approach to determine information security requirements to ensure that security is commensurate with the risk and magnitude of harm that can result from the loss, misuse, unauthorized access to, or modification of, OPIC information.

   (b) OPIC management will make all information technology decisions based on a thorough analysis of the risks involved.

   (c) Risk management procedures must be integrated into OPIC's systems development life cycle (SDLC). Risk management is an iterative process and has activities relevant to every phase of the life cycle. Security considerations must be included in the initiation, development/acquisition, implementation, operation/maintenance, and disposal of all OPIC information resources.

   (d) Risk management is a cyclical process and must be performed on an ongoing basis for all information resources.

(e) OPIC will adhere to NIST guidance as set forth in Special Publication 800-30, Risk Management and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners and OPIC Executives are responsible for:

(1) Committing to performing on-going periodic risk management of information resources.

(2) Considering the results of a risk assessment in making decisions about the use of information resources.

(3) Implementing appropriate safeguards based on the results of risk analysis.

(b) Information Custodians are responsible for:

(1) Assisting with the assessment and mitigation of risks for the information resources with which they have been entrusted.

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

(1) Developing OPIC risk management procedures.

(2) Conducting risk assessments on OPIC information systems.

(3) Identifying potential threats to the confidentiality, integrity, and availability of OPIC information resources.

(4) Performing vulnerability testing in accordance with OPIC policies and procedures.

(5) Providing recommendations for the cost-effective mitigation of risks to information resources.

6. DEFINITIONS:

(a) Availability - Assuring information and communications services will be ready for use when expected

(b) Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

(c) Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete, and consistent.

(d) Risk – The possibility of something adversely affecting the confidentiality, availability and integrity of OPIC's information resources.

(e) Risk Assessment - The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk.

(f) Risk Management – The process of identifying risk, assessing riskRisk, and taking steps to reduce risk to an acceptable level. The risk management process allows OPIC to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support the agency's mission.

(g) Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

(h) Vulnerability – Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

(i) Vulnerability Testing – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

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

(e) NIST Special Publication 800-30, Risk Management.

(f) 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.

SECURITY TRAINING AND AWARENESS

ISSP-04-0410

1. **SUBJECT:** OPIC's information security policies and procedures will be communicated to all employees. They will be made available for reference and review by employees and any other persons who are in positions that can impact the security and integrity of OPIC information resources. A program to maintain effective awareness of information security policy, standards and acceptable practices will also be implemented. Additionally, persons responsible for administering or securing information resources must have adequate training on the proper implementation of security controls for the systems and data under their control.

2. **SCOPE:** This policy applies to all OPIC employees and contractors, including interns and temporary workers, who have access to OPIC information resources. The term "employees" will be used in this policy to specify all personnel within this scope.

3. **DESCRIPTION:** The Federal Information Security Management Act (FISMA) requires each federal agency to provide mandatory periodic information security training to all employees involved in the use or management of federal computer systems. Further, the Office of Management and Budget (OMB) Circular A-130 requires that such training be completed prior to the granting of access, and be provided for periodic refreshment.

   Aside from compliance with legal requirements, a Security Training and Awareness program is crucial to the safeguarding of OPIC information resources. Information security policy and standards cannot be effective unless everyone at OPIC, regardless of position in the organization, is aware of the importance of security, understands OPIC security procedures, and performs required practices. To make information security effective, standards and procedures must be known, understood, believed to be beneficial, and be appropriately and consistently practiced.

   Information Security is not a one-time event, but a continuous effort and "state of mind". This is achieved by reinforcing concerns and appropriate behaviors on a continuous basis. Effective information security is achieved when it becomes part of everyone's thinking with regard to daily operations and assignments.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will develop and maintain an Information Security Training and Awareness Program to educate employees about information security policies and procedures, and make them aware of their roles and responsibilities in safeguarding OPIC's information resources. The program will be composed of two major initiatives:

   (1) A Training program designed to build relevant and needed security skills and competencies to facilitate job performance.

(b) An Awareness program designed to focus attention on security, and to change behavior or reinforce good security practices. Ongoing development of security awareness builds a culture that encourages good security practices.

(c) All information users will complete training on OPIC Information security policies and procedures. This will consist of three (3) training activities:

(1) Information security training will be incorporated into the orientation processes for all new staff. Training must be completed within 30 days of employment or initiation of contract.

(2) All information users will complete an annual Information security training program to refresh their knowledge of information security.

(3) Information Custodians and other personnel with responsibilities related to administering and securing systems will be provided with enhanced security training applicable to their functions.

(d) OPIC will maintain and publish an Information Security Handbook documenting policies, procedures, and responsibilities.

(e) On an annual basis, employees will sign an agreement that they understand the OPIC Information security policies and procedures and that they will abide by them.

(f) Employees will be made aware of the penalties for non-compliance with OPIC security policies and procedures.

(g) Materials will be posted or presented in a variety of formats on a regular basis to maintain user awareness of information security issues.

(h) Changes to OPIC Information security policies or procedures will be communicated to all information users.

(i) OPIC will adhere to NIST guidance as set forth in NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) The Information Systems Security Officer (ISSO) is responsible for developing and operating the Information Security Training & Awareness program, including:

(1) preparing policy on security awareness and training,

(2) developing and presenting security training courses and briefings,

(3) developing and distributing awareness material and bulletins, and ensuring all personnel receive the appropriate security training associated with their jobs, and

(4) maintaining records of training received.

(b) Supervisors and COTRs are responsible for:

(1) Ensuring that their employees are briefed and understand their roles in implementing OPIC's Information Security program.

(2) Communicating changes in policies and procedures to their staff.

(3) Providing opportunities for staff to complete information security training.

(4) Assisting with the monitoring of information security compliance within their departments.

(c) Information Users are responsible for:

(1) Completing annual security training.

(2) Reviewing and understanding OPIC information security policies and procedures.

(3) Completing and abiding by the "Agreement To Comply With OPIC Information Security Policy" document.

(4) Complying with all OPIC information security policies and procedures.

(d) Information Owners are responsible for ensuring that personnel who use their resources are appropriately trained to fulfill their security responsibilities for those resources.

6. **DEFINITIONS:**

(a) Awareness – A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.

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:

(a) Agreement To Comply With OPIC Information Security Policy

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

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

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(f) Computer Security Act of 1987, PL 100-235, January 8, 1988.

(g) NIST Special Publication 800-50, Building an Information Technology Security Training and Awareness Program.

(h) 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.

Agreement to Comply With OPIC Information Security Policy

OPIC is committed to information security and employs specialists to maintain security. However, it is the responsibility of users to comply with all information security policies and procedures. By signature below, the employee or contractor hereby acknowledges and agrees to the following:

1. The employee or contractor is a “user” as defined in the OPIC information security policy handbook.
2. As a user, he/she shall comply with security measures prescribed by the OPIC information security policies.
3. The user shall protect OPIC information resources in his/her possession from unauthorized activities including disclosure, modification, deletion, and misusage.
4. The user agrees that they will only obtain, use, or disclose information in an authorized fashion and for authorized purposes.
5. The user has read and agrees to abide by OPIC’s information security policies and the “OPIC Information Security Handbook.”
6. The user agrees to discuss with his/her OPIC supervisor any policies or procedures not understood.
7. Access to OPIC information systems is a privilege that may be changed or revoked at the discretion of management.
8. Access to OPIC information systems automatically terminates upon termination of OPIC employment.
9. The user shall promptly report any suspected violations of OPIC security policies to the Information Systems Security Officer (ISSO).
10. This document may be amended from time to time. OPIC will notify users of amendments. Users will keep abreast of amendments as made available.

The user understands that anyone found to violate these policies is subject to disciplinary and/or legal action, including but not limited to:

1. Loss or limitation of use of information resources
2. Termination of employment
3. Referral for criminal prosecution.

ACKNOWLEDGMENT: OPIC INFORMATION TECHNOLOGY POLICY

______________________________________ ____________________

User’s signature Date

______________________________________ Employee / Contractor

Print User’s Name (circle one)

Elevated Privileges/Information Custodian Agreement

It is the responsibility of all OPIC information users to comply with information security policies and procedures. Persons entrusted with responsibilities for administering information systems have a particularly important role in protecting these systems. By signature below, the employee or contractor hereby acknowledges and agrees to the following:

1. The employee or contractor is an “information custodian” (custodian) as defined in the “OPIC Information Security Handbook.”
2. The custodian acknowledges that he/she has been granted enhanced privileges in order to perform specific administrative functions on specific OPIC information systems, and that these privileges are only to be used in order to perform his/her assigned job responsibilities.
3. The custodian will not use his/her privileges to grant him/herself or any other persons unauthorized privileges, or to modify any access accounts, privileges, system configurations, or data in an unauthorized manner.
4. The custodian accepts that he/she has a special duty to safeguard OPIC information resources, and will implement and operate appropriate measures to protect those resources.
5. The custodian will exercise maximum care in protecting the enhanced access credentials with which he/she has been entrusted.
6. The custodian has read and agrees to abide by OPIC’s information security policies and the “OPIC Information Security Handbook,” especially those rules that apply to information custodians.
7. Access privileges to OPIC information systems may be changed or revoked at the discretion of management, and may be modified as roles and responsibilities change.
8. In addition to this agreement, the custodian will also sign and abide by the “Agreement to Comply With OPIC Information Security Policy” document.
9. This document may be amended from time to time. OPIC will notify custodians of amendments. Custodians will keep abreast of amendments as made available.

The custodian understands that anyone found to violate these policies is subject to disciplinary and/or legal action, including but not limited to:

1. Loss or limitation of use of information resources,
2. Termination of employment, and/or
3. Referral for criminal prosecution.

ACKNOWLEDGMENT: OPIC INFORMATION TECHNOLOGY POLICY

____ ________________________

Information Custodian’s Signature Date

____ Employee / Contractor

Print Information Custodian’s Name (circle one)

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.

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.

SYSTEM SECURITY PLANS

ISSP-07-0410

1. **SUBJECT:** Each major information system must have an approved security plan.

2. **SCOPE:** This policy covers all major OPIC information systems.

3. **DESCRIPTION:** A security plan lists security requirements, defines risks, and describes security measures to be implemented for a particular system. This helps to ensure that a security risk analysis is performed for the system, and that appropriate security controls are put in place. The security plan also defines roles and responsibilities for security of the system, as well as standard operating procedures.

4. **PROCEDURES & GUIDELINES:**

   (a) Each new major information system must have an approved Security Plan before going into operation.

   (b) Owners of existing major information systems that do not have an approved Security Plan must develop one as soon as possible.

   (c) Each System Security Plan must be reviewed, updated, and re-approved at least once every two years, or when there is a major change to the system, whichever is earlier.

   (d) The System Security Plan will be used as a critical component of the Certification and Accreditation of the system.

   (e) Other organizations or systems that are connected to or share data with the OPIC system must have a Memorandum of Understanding (MOU) or other formal documented agreement that describes the rules governing the interconnection.

   (f) System Security Plans must be marked, handled, and controlled as sensitive but unclassified information.

   (g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for:

   (1) Ensuring that System Security Plans are developed for the systems that they own.

   (2) Formally approving and accepting system security plans for their systems.

   (b) Information Custodians are responsible for assisting Information Owners and the ISSO with the development and implementation of System Security Plans.

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

   (1) Assisting with the development and review of system security plans.

(2) Auditing systems to ensure that their security plans have been effectively implemented.

6. DEFINITIONS:

(a) Major Information System – An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

(b) Memorandum of Understanding (MOU) - A document providing a general description of the responsibilities that are to be assumed by two or more parties in their pursuit of some goal(s).

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

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

(e) OMB Circular A-123, Internal Control Systems, August 4, 1986.

(f) NIST Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems.

(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.

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.

VULNERABILITY TESTING

ISSP-09-0410

1. **SUBJECT:** In order to assess OPIC's information security posture and determine the security risks that should be mitigated, OPIC will conduct periodic vulnerability assessments. These assessments will assist in the discovery of security vulnerabilities, gauge the threat posed by these vulnerabilities, and assist OPIC with decreasing security risk.

2. **SCOPE:** This policy applies to all OPIC owned or operated systems, networks, applications, data repositories, and other information resources.

3. **DESCRIPTION:** Today's information systems are complex and composed of many interdependent and interconnected components. No matter how well they have been developed, all systems have some inherent vulnerabilities or exploitable flaws. Over time, these vulnerabilities are likely to be exploited, either intentionally or accidentally.

   Security testing is an important means of detecting weaknesses and determining the threat posed by them. It also helps to determine the effectiveness of security measures that have been implemented, and to assess how well the organization can withstand security attacks. A vulnerability testing program provides the crucial details to prepare OPIC to avoid the significant financial costs or damage to its reputation that could result from security malfeasance.

   Because threats, vulnerabilities, and the configurations of the systems themselves are always changing, the Federal Information Security Management Act (FISMA) requires OPIC to perform security testing on a periodic basis. A systematic, comprehensive, ongoing, and priority-driven security testing program will assist OPIC with determining its security priorities and making prudent investments to enhance the security posture of its information resources.

4. **PROCEDURES & GUIDELINES:**

   (a) Vulnerability testing should be conducted at least annually while systems are running in their operational environments.

   (b) Testing should not disrupt critical business operations.

   (c) Procedures for testing should be clearly defined and documented.

   (d) All test results should be well documented.

   (e) If necessary, the "rules of engagement" should be communicated to the system owners.

   (f) Information Owners and Information Custodians should be informed of the results to ensure that vulnerabilities are patched or mitigated.

   (g) All systems should be retested once vulnerabilities are addressed to ensure that they have been effectively mitigated.

(h) Vulnerability testing should be integrated into OPIC's risk management processes.

(i) OPIC will adhere to NIST guidance as set forth in Special Publications 800-42, Guideline on Network Security Testing; 800-51, Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme; 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems, and subsequent publications, as well as other relevant best practices.

5. ROLES & RESPONSIBILITIES:

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

(1) Developing testing procedures.

(2) Performing periodic testing.

(3) Documenting test results.

(4) Communicating vulnerabilities to Information Owners and Custodians.

(5) Auditing to ensure that vulnerabilities have been mitigated.

(6) Providing advice to Information Owners and Custodians regarding potential mitigation strategies.

(b) Information Owners are responsible for:

(1) Allowing vulnerability testing to be performed on their resources.

(2) Ensuring that any identified vulnerabilities are resolved for their resources.

(c) Information Custodians are responsible for:

(1) Assisting the ISSO with performing security testing, as requested.

(2) Helping Information Owners with selecting and implementing mitigation strategies.

(3) Documenting mitigations that are implemented.

(4) Informing the ISSO about mitigations performed.

6. DEFINITIONS:

(a) Threat - A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

(b) Vulnerability– Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

(c) Vulnerability Assessment (or Vulnerability Testing) – Systematic examination of a system to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

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) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(e) NIST Special Publication 800-42, Guideline on Network Security Testing

(f) NIST Special Publication 800-53A, Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems

(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.

CONTINGENCY PLANNING

ISSP-10-TBD

1. **SUBJECT:** OPIC will establish a comprehensive and effective program to ensure continuity of essential agency functions during a broad spectrum of emergencies or situations that may disrupt normal operations.
2. **SCOPE:** This policy applies to all major information systems and mission-critical applications.
3. **DESCRIPTION:** In addition to being a legal mandate for federal agencies, contingency planning is simply a good business practice, and part of the fundamental mission of OPIC as a responsible and reliable public institution. For the success of OPIC's programs, the agency's information systems must be available in the event of disruptions.

   OPIC's information systems are vulnerable to a variety of disruptions, ranging from mild (*e.g.*, short-term power outage) to severe (*e.g.*, equipment destruction, fire), and from a variety of sources ranging from natural disasters to terrorists actions. While many vulnerabilities may be minimized or eliminated through technical, management, or operational solutions as part of OPIC's risk management program, it is virtually impossible to completely eliminate all risks. In many cases, critical resources reside outside OPIC's control (such as electric power or telecommunications), and the agency may be unable to ensure their availability. Thus effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.
4. **PROCEDURES & GUIDELINES:**

   (a) OPIC will develop and maintain a viable contingency planning program for its major information systems and mission-critical applications.

   (b) The program will support OPIC's agency-level Continuity of Operations (COOP) Planning.

   (c) The program will yield documented plans on how OPIC would continue its mission and provide continuity of data processing if service, use, or access was disrupted for an extended period of time.

   (d) Each major IT system will have its own Contingency Plan, Continuity of Support Plan, or Disaster Recovery Plan.

   (e) Contingency planning will be based on business impact analyses that will identify and rank major information systems and mission-critical applications according to priority and the maximum permissible outage for each.

   (f) Preventive measures will be identified to reduce the effects of system disruptions and increase system availability.

   (g) Recovery strategies and procedures will be developed to ensure that systems may be recovered quickly and effectively following a disruption.

(h) Contingency plan testing and training will be held to address deficiencies and to prepare Information Owners and Custodians for plan activation.

(1) Testing will occur annually or when a significant change occurs to OPIC's major information systems or mission-critical applications.

(i) Contingency plans will be reviewed regularly and updated as needed to remain current with OPIC information technology enhancements.

(j) OPIC will adhere to NIST guidance as set forth in Special Publication 800-34, Contingency Planning Guide for Information Technology Systems and subsequent publications.

5. ROLES & RESPONSIBILITIES:

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

(1) assisting in identifying major information systems and mission critical applications.

(2) reviewing contingency plans to ensure they align with the overall agency COOP plan and information security policies.

(3) providing training, support and coordination for Information Owners and Custodians as they develop and coordinate contingency plans.

(4) ensuring that contingency plans are updated and tested annually.

(5) monitoring the contingency planning process and reporting progress to management as required.

(6) maintaining current copies of all contingency plans, tests, evaluations, and subsequent follow-up actions and making this information available as required.

(7) activating and coordinating established contingency plans during an emergency.

(b) Information Owners are responsible for:

(1) developing, reviewing, and testing system and application contingency plans for the resources they own.

(2) developing a strategy for providing adequate alternate processing capability based on the prioritization of major systems or critical applications which they own.

(3) providing personnel for contingency plan testing

(4) maintaining a list of the personnel involved in the disaster planning/recovery process, including their functions, roles, and assigned tasks.

(c) Information Custodians are responsible for:

(1) working with Information Owners and the ISSO to develop contingency plans.

(2) participating in contingency plan testing.

6. **DEFINITIONS:**

(a) Contingency Plan – Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, sys tem failures, or disaster.

(b) Continuity of Support Plan (COSP) – The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.

(c) Continuity Of Operations Plan (COOP) – A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

(d) Disaster Recovery Plan (DRP) – A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

(e) Disruption – An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

(f) Major Information System – An information system that requires special management attention because of its importance to an agency mission (and in this case mission critical business processes).

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) Presidential Decision Directive 67, Continuity of Operations, October 21, 1998.

(e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(f) NIST Special Publication 800-34, Contingency Planning Guide for Information Technology Systems

(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.

ACCESS CONTROL

ISSP-11-0410

1. **SUBJECT:** Access to OPIC information resources will be limited to those that need those resources to perform their duties. The principles of separation of duties and least privilege will be applied to the allocation of access rights.
2. **SCOPE:** This policy applies to all OPIC information users, owners, and custodians, as well as access to any OPIC information resources.
3. **DESCRIPTION:** Users must have access to the information resources required to do their jobs. However, excessive or uncontrolled access can lead to the unauthorized or unintentional disclosure, modification, or destruction of those resources, as well as liability for negligence in protecting those resources. Therefore, access to specific resources is only to be granted to authorized personnel who have a legitimate need to use those resources, and their access privileges will be limited to those required to perform their duties.
4. **PROCEDURES & GUIDELINES:**

(a) Users must be granted specific access privileges on each system, limited to those required to perform their job functions.

(b) Users must be authorized by the information owner prior to being granted access to a particular resource.

(c) Users will only access resources to which they have been authorized, regardless of actual system permissions.

(d) Users will not circumvent the permissions granted to their accounts in order to gain access to unauthorized information resources.

(e) Users will protect their own accounts:

(1) Users will not allow anyone else to use their account, or use their computers while logged in under their account, except as required for system administration.

(2) When leaving their computer unattended, users will either log out or invoke protection of their system (such as a password-protected screensaver).

(3) Users are responsible for any activity initiated by their own userID (since only they should have access to their userID).

(f) The level of access control will depend on the classification of the resource and the level of risk associated with the resource.

(g) Criteria must be established for account eligibility, creation, maintenance, and expiration for each system.

(h) Information Custodians (i.e. system administrators) will periodically review user privileges and modify, revoke, or deactivate as appropriate, based on the above criteria.

(i) Inactivity timeouts will be implemented, where technically feasible, for access to sensitive information.

(j) Employee access to OPIC information systems will be limited to standard OPIC business hours, unless otherwise permitted by IRM for legitimate business purposes. Employees will not be permitted access to OPICNET during nightly scheduled backup periods.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for:

(1) Determining who should have access to their resources.

(2) Ensuring that their resources are protected against unauthorized access.

(3) Periodically reviewing access permissions.

(4) Ensuring that information users have undergone appropriate background checks and security training.

(b) Information Custodians are responsible for:

(1) Assisting information owners with controlling access to their resources.

(2) Promptly removing access from a system when requested.

(3) Reporting any unauthorized accesses that they discover.

(c) Information Users are responsible for:

(1) Understanding OPIC information resource access policies and procedures.

(2) Adhering to OPIC procedures for obtaining and removing access to information resources for themselves.

(3) Safeguarding their access credentials.

(4) Accessing only those resources for which they are authorized and using information in accordance with job function and agency policy.

(5) Immediately reporting suspected violations of this policy to their supervisor or the ISSO.

(6) Understanding the consequences of their failure to adhere to this policy.

(d) Supervisors are responsible for:

(1) Adhering to OPIC procedures for obtaining and removing access to information resources for their employees, contractors, and interns.

(2) Ensuring that their employees are authorized to access the resources needed to perform their duties.

(3) Notifying the ISSO when access privileges or accounts are to be removed.

(4) Immediately reporting suspected violations of this policy.

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

(1) Auditing to ensure compliance with the procedures and guidelines specified in this policy.

(2) Ensuring that all personnel are trained on their computer security responsibilities.

(f) The OPIC Security Officer is responsible for ensuring that IT staff and IT contractors have undergone the appropriate background checks and security training.

6. **DEFINITIONS:**

(a) Access – The right to enter, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of specific information resources.

(b) Access Control – The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

(c) Access Privilege (Privilege) – A specific activity that a user has been granted access to perform on an information resource (e.g. view or modify)

(d) Account – A set of privileges for authorization to system access, which are associated with a UserID.

(e) Authorization – The formal granting of access to an individual to perform certain activities.

(f) Least Privilege – Granting users only the minimum privileges required to provide the level of access needed to perform their official duties.

(g) Separation of Duties – Concept that provides the necessary checks and balances to mitigate against fraud, errors and omissions by ensuring that no individual or function has control of the entire process.

(h) System Permissions – The technical configuration that provides an individual the ability to perform certain actions on information resources.

(i) UserID – Character string (i.e. logon name) that uniquely identifies a computer user.

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) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(e) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(f) 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.

IDENTIFICATION AND AUTHENTICATION

ISSP-12-TBD

1. **SUBJECT:** Access to OPIC information systems will only be granted to identified and authenticated users. OPIC will establish procedures and controls for granting, changing, and terminating access to information systems.
2. **SCOPE:** This policy applies to all OPIC owned or operated information systems, both operational and in development.
3. **DESCRIPTION:** In order to ensure that unauthorized persons do not have access to sensitive OPIC information resources, it is necessary to first establish the identity of the user who is attempting to access the resource. Access controls can then be used to allow or limit access based on the established user identity.

   The specific method(s) of authentication used for each system shall be commensurate with the level of sensitivity of the system to be accessed (*i.e.* more sensitive systems should use stronger authentication methods). Multiple authentication methods (*e.g.* use of both a password and a token) may be required for high-sensitivity or high-risk situations.
4. **PROCEDURES & GUIDELINES:**

   (a) Each OPIC system shall incorporate proper user authentication and identification to ensure that access is not granted to unauthorized persons. Users will not have access to OPIC information resources without identifying and authenticating themselves (*i.e.* "logging on").

   (b) OPIC will develop and follow detailed procedures for the creation, removal, and modification of user accounts and authentication credentials.

   (c) User accounts must adhere to the following guidelines:

   (1) Allow only one user per account; User IDs are never to be shared.

   (2) Never install a guest/guest account. Remove any guest accounts that are created by default by the system unless absolutely required approved by the system owner and the ISSO.

(3) No accounts will be named with easily guessed generic names (such as “anonymous”, “guest”, “admin”, “ftp”, “telnet”, “www”, “host”, “user”, “test”, “bin”, “nobody”, etc.) unless absolutely technically required by the system.

(4) Default accounts that are present upon initial installation of the system should be removed or renamed unless absolutely technically required by the system.

(5) Accounts should be deactivated immediately upon termination of an employee or contractor.

(6) Unused accounts will be deactivated on at least a monthly basis.

(7) Accounts for contractors and temporary employees should expire on the final date of their contract.

(b) Administrator accounts must adhere to the following guidelines:

(1) The names of the administrator accounts should be renamed, if possible, to make it more difficult for attackers to guess the names of these accounts.

(2) Each person who has a legitimate need to use Administrator privileges should have their own administrative account that they will use to perform administrative functions. Usage of the main administrator account for each system should be limited to emergencies, and is to be limited to designated IRM staff. This will protect the main administrator account and also provide an audit trail of administrative activities.

(3) All accounts with administrator privileges should have strong passwords or other alternative strong authentication methods.

(d) If passwords are used for authentication, they must adhere to the OPIC Password Management policy.

(e) If authentication methods other than passwords other than passwords (e.g., biometrics, smartcards, tokens, etc), then:

(1) They must be approved by the ISSO.

(2) Additional policies and procedures will be developed to govern their usage.

(f) Account credential information (e.g., User IDs, passwords) that are stored on the devices (such as enable passwords in router configuration files) must be encrypted.

(c) To preclude brute force attacks, an intruder lockout feature should be implemented on each system to temporarily suspend the account after three invalid logon attempts. Manual action by a security system administrator is required to reactivate the ID.

(d) OPIC will restrict access to authentication data. Authentication data will be protected with access controls and encryption to prevent unauthorized individuals from obtaining the data.

(e) OPIC will adhere to NIST guidance as set forth in NIST Special Publication 800-63, Recommendations for Electronic Authentication, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Employees shall understand their responsibilities for safeguarding User IDs and passwords, and immediately notify a supervisor or the Information Custodian (e.g., the IRM department) if they suspect that a password or other system credential has been compromised.

(b) Supervisors shall ensure that their personnel understand and comply with the guidelines contained in this policy, promptly notify Information Custodians of accounts that should be deactivated, and report any suspected violations or compromises of credentials to the ISSO and the Information Custodian.

(c) Information Custodians shall implement appropriate identification and authentication methods for the information resources in their care, instruct users as to their usage, and report any compromises of these resources to the ISSO and the Information Owner.

(d) Information Owners shall ensure that appropriate identification and authentication methods are implemented for the resources that they own, based on the classification and level of risk assigned to the resource.

(e) The Information Systems Security Officer (ISSO) shall prepare guidelines and standards for user credentials, perform compliance reviews, and approve issuance of administrator credentials.

(f) System Developers must ensure that their systems support the procedures and guidelines specified in this policy document.

6. DEFINITIONS:

(a) Authentication – The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(b) Brute Force Attack - attack where the attacker attempts to systematically "guess" a password or other secret by trying all possible values.

(c) Identification – The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, "jsmith").

(d) Information Resources – The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

(e) Password – Any secret string of characters which serves as authentication of a person's identity, and which may be used to grant or deny access.

(f) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.

(g) User ID - Character string that uniquely identifies a computer user or computer process.

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) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.

(d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.

(e) NIST Special Publication 800-63, Recommendations for Electronic Authentication.

(f) 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.

AUDIT TRAILS

ISSP-13-0410

1. **SUBJECT:** Audit trails must be maintained to provide accountability for the use of OPIC's information resources.
2. **SCOPE:** This policy applies to all OPIC information systems and all information users.
3. **DESCRIPTION:** In order to enforce information usage policies and security measures, and to be able to investigate security incidents, automated logs of access to and alteration of information systems and data must be maintained. To accomplish this, a record of activity (or "audit trail") of system and application processes and user activity of systems and applications must be maintained. This is used to investigate security incidents, monitor use of OPIC resources, provide accountability for transactions, track system changes, and assist in detection of system anomalies. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.
4. **PROCEDURES & GUIDELINES:**

   (a) Audit Trails will be maintained for OPIC information systems:

   (1) At minimum, the following transactions should be logged for each server:

   - Server startup and shutdown
   - Loading and unloading of services
   - Installation and removal of software
   - System alerts and error messages
   - User logon and logoff
   - System administration activities
   - Accesses to sensitive information and systems
   - Modifications of privileges and access controls
   - Additional security related events

   (2) At minimum, the following transactions should be logged for each application:

   - Modifications to the application
   - Application alerts and error messages
   - User sign on and sign off
   - System administration activities

- Accesses to sensitive information
- Modifications of privileges and access controls

(3) At minimum, the following transactions should be logged for each router, firewall, or other major network device:

- Device startup and shutdown
- Administrator logon and logoff
- Configuration changes
- Account creation, modification, or deletion
- Modifications of privileges and access controls
- System alerts and error messages

(4) Type of event, date, time, and user identification must be recorded for each logged transaction.

(5) Sensitive information, such as passwords and actual system data, should not be stored in the logs.

(b) Periodic reviews of audit logs will be conducted by the ISSO or other designated personnel.

(c) Only designated personnel should have access to the audit logs.

(d) Audit trail files are to be kept for at least one (1) year.

(1) Audit trails associated with known incidents (including those used for legal action) are to be kept for three (3) years.

(e) Audit trails must be kept in a secure location. Audit data should be some of the most carefully secured data at the site and in the backups. If an intruder were to gain access to audit logs, the systems themselves, in addition to the data, would be at risk.

(f) OPIC will follow NIST guidance regarding audit trails.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that audit trails are implemented and maintained for their resources.

(b) Information Custodians are responsible for assisting information owners with implementing and maintaining audit trails for the resources for which they are responsible.

(c) Supervisors are responsible for assisting the ISSO in reconciling audit trail anomalies.

(d) The Information Systems Security Officer (ISSO) is responsible for periodically reviewing audit trails for all systems to ensure compliance with this policy.

(e) Information Users are responsible for understanding and acknowledging that their use of OPIC systems may be logged and audited.

6. DEFINITIONS:

(a) Audit Trail - In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

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

(d) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(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.

ANTIVIRUS

ISSP-14-0410

1. **SUBJECT:** Standard software and procedures must be implemented to minimize the impact of computer viruses on OPIC's information resources.

2. **SCOPE:** This policy applies to all OPIC servers and workstations, as well as any computers used for remote access to the OPIC network. Exceptions may be granted for operating systems that do not have readily available virus detection software.

3. **DESCRIPTION:** Computer viruses are programs that reproduce themselves and often attempt to do harm to the computers that they infect. Viruses may destroy OPIC data, make OPIC computers unusable, use OPIC's computer to attack other computers, or perform a variety of other malicious activities. There are many different types of computer viruses.

   Use of antivirus software is essential for protecting OPIC resources from the danger posed by computer viruses and other malicious programs. These programs check for viruses on OPIC's computers and attempt to remove them before they can spread or perform further damage.

   However, antivirus programs take time to learn about each new virus that is created, during which the virus can do serious damage. Therefore, it is also important that users and system administrators be aware of the risks posed by viruses, and take steps to minimize exposure to them.

4. **PROCEDURES & GUIDELINES:**

   (a) Every OPIC server and workstation must run the agency standard, supported antivirus software.

   (b) OPIC will use antivirus software at its email gateway to scan messages and attachments.

   (c) Employees may not unload or disable antivirus software for any reason without specific instruction from IRM.

   (d) Antivirus software is to be updated automatically as new virus profiles are made available by the vendor.

   (e) Any computer used for remote access to the OPIC network (such as a laptop used for telecommuting or a home computer used to do OPIC work) must have approved antivirus software loaded and updated on a regular basis.

   (f) Any infected files that cannot be repaired must be quarantined or deleted.

   (g) Any infected computers that cannot be cleaned by the antivirus software must be removed from the network until they can be verified as virus free.

   (h) Employees are to be trained on techniques for avoiding viruses, including the following guidance:

(1) Never open any files attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately and empty your Trash.

(2) Delete spam, chain, and other junk email without forwarding.

(3) Never download files from unknown or suspicious sources.

(4) Never install any software on OPIC computers without specific permission from IRM.

(i) All portable media (*e.g.* floppy diskettes, CDs) must be scanned for viruses before use on an OPIC computer.

(j) If lab testing conflicts with antivirus software, run the antivirus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the antivirus software. When the antivirus software is disabled, do not run any applications that could transfer a virus, *e.g.*, email or file sharing.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for deploying antivirus software and procedures on any servers or workstations that they own.

(b) Information Custodians are responsible for assisting information owners with the implementation of antivirus software and procedures.

(c) Information Users are responsible for taking appropriate precautions to avoid introducing viruses into the OPIC computing environment.

(d) Supervisors are responsible for assisting their employees with understanding and complying with OPIC antivirus procedures and guidelines.

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

(1) Auditing the OPIC computer environment for adherence to this policy.

(2) Ensuring all personnel are trained on the application of this policy.

6. **DEFINITIONS:**

(a) Antivirus software– commercially available software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus may have caused.

(b) Remote Access – Any access to OPIC's corporate network through a network, device, or medium that is not controlled by OPIC (such as the Internet, public phone line, wireless carrier, or other connectivity).

(c) Virus – A malicious program which, when executed, copies itself onto other media or files available to the computer executing it and may cause damage to a computer system by attacking or attaching itself to boot information, email, data file, or another program.

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) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(d) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(e) Homeand Security Presidential Directive / HSPD-7, December 17, 2003

(f) 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.

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.

PHYSICAL AND ENVIRONMENTAL SECURITY

ISSP-17-0410

1. **SUBJECT:** Information resources require physical security measures to ensure proper and timely operation, to protect value, to safeguard the integrity of information, and to ensure the safety of personnel. Computer systems, facilities, and tape storage areas shall be protected from theft, alteration, damage by fire, dust, water, power loss and other contaminants, and unauthorized disruption of operation.

2. **SCOPE:** This policy prescribes the procedures, guidelines, and standards that govern the implementation of physical security measures designed to protect OPIC information resources. It does not govern protection of personnel, facilities, and property not directly associated with information technology, which are covered by OPIC Directive 94-14.

3. **DESCRIPTION:** It is crucial that OPIC implement physical security safeguards to protect its information resources. These safeguards must be applied in all administrative, physical, and technical areas and can include the use of locks, guards, administrative controls, and measures to protect against damage from intentional acts, accidents, fires, and environmental hazards.

4. **PROCEDURES & GUIDELINES:**

   (a) Physical access to information resources is to be controlled commensurate with the classification of the resource and the level of risk.

   (b) Areas containing sensitive information resources require special restrictions to limit access to these resources:

      (1) Admittance to these areas is to be limited to personnel assigned to the area and persons who have been specifically authorized access to the area.

      (2) Personnel assigned to the area must escort personnel without an appropriate security clearance.

      (3) When uncleared personnel are present in these areas, sensitive information must be protected from observation, disclosure, or removal. This includes storing away documents and positioning all computer monitors to prevent viewing by unauthorized persons.

      (4) Each person within a sensitive area, regardless of position, shall be subject to challenge by another OPIC employee, facility security personnel, or any law enforcement officer, and shall display appropriate identification when challenged. Failure to do so may result in removal from the facility or other administrative action.

      (5) Areas containing sensitive information must be physically secured in accordance with OPIC facility security policies and OPIC Directive 94-14.

   (c) Areas containing critical information resources require special protections to safeguard the availability of these resources:

(1) Protection must be implemented against fire, flood, humidity, electromagnetic disturbance, and other environmental factors that could damage the resources.

(2) Automated systems should monitor for environmental problems and alert specified personnel as appropriate.

(3) Smoke and fire detection systems with alarms must be installed in accordance with OPIC facility security policies and OPIC Directive 94-14.

(d) Specific requirements for the Computer Room (*i.e.*, "Data Center"):

(1) Comply with all requirements listed above.

(2) Install fire suppression equipment.

(3) Provide emergency power shutdown controls. Cover controls to prevent accidental activation.

(4) Equipment is to be located on a raised floor

(5) Provide an uninterruptible power supply

(6) Vendors and visitors are to be escorted at all times.

(7) All physical access to the room must be tracked.

(8) Annual testing will be performed on all fire, utility, and environmental alarms and protective systems.

(e) Backups and other media, both originals and copies, containing data and programs must be kept in good condition and protected from theft. It is important to keep backups in a separate location from the originals, not only for damage considerations, but also to guard against thefts.

(f) Other areas where physical access should be restricted are wiring closets and computer storage areas.

5. ROLES & RESPONSIBILITIES:

(a) Information Users are responsible for:

(1) Understanding and adhering to the security requirements prescribed in this policy

(2) Physically protecting the OPIC information resources entrusted into their possession.

(3) Reporting any incident or condition contrary to the specified requirements to the ISSO or OPIC Security Officer.

(b) Supervisors are responsible for:

(1) Ensuring that their personnel understand OPIC policy regarding physical and environmental security.

(2) Monitoring their employees' compliance with this policy.

(c) Information Owners are responsible for implementing measures to protect their resources aga inst physical and environmental threats, as well as unauthorized physical access.

(d) Information Custodians are responsible for assisting information owners with implementing physical and environmental security measures.

(b) The Information Systems Security Officer (ISSO) is responsible for performing auditing to ensure compliance with these policies and guidelines.

(c) The OPIC Security Officer is responsible for ensuring the physical and environmental security of the OPIC facilities.

6. DEFINITIONS:

(a) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

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

(a) **AUTHORITY:** 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 800-26, Security Self-Assessment Guide for Information Technology Systems.

10. LOCATION: TBD

11. EFFECTIVE DATE: October 22, 2004

12. REVISION HISTORY: None

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

CHANGE CONTROL

ISSP-18-0410

1. **SUBJECT:** Authorized changes must occur to OPIC's network and information systems, and these changes must occur in a timely manner without disruption or compromise to existing system operation. However, OPIC must protect its information systems from unauthorized changes, intrusions or misuse. One way of facilitating this requirement is to formally manage and control hardware and software configuration changes.

2. **SCOPE:** This policy applies to all OPIC information systems.

3. **DESCRIPTION:** Change control involves controlling and managing changes to OPIC's information systems to ensure integrity of data and information. OPIC information systems require appropriate administrative, physical and technical controls to be incorporated into both new additions and changes to systems. These controls must encompass not only the software, but also the routine activities that enable OPIC's information systems to function properly (*e.g.*, fixing software or hardware problems, loading and maintaining software, updating hardware and software, and maintaining a historical record of application changes). Change control prevents unexpected changes from inadvertently leading to denial of service, unauthorized disclosure of information, and other problems.

   Informal operational processes with no means of controlling changes to information systems impede OPIC's ability to determine the status of its current architecture, network component configuration and even to propose changes. Change control planning addresses this deficiency and establishes a consistent, cross-organizational change management process for OPIC information systems. Change control history lays the framework of how OPIC's network is built and is a valuable tool for both emergency response and information architecture planning.

4. **PROCEDURES & GUIDELINES:**

   (a) Changes to each OPIC information system will be systematically planned, approved, tested and documented at a level appropriate with the size, complexity, and sensitivity of the system.

   (b) OPIC will develop baseline information that includes a current list of all components (hardware, software, and their documentatio n), configuration of peripherals, version releases of current software, information on batch files, environmental settings such as paths, and switch settings of machine components.

   (c) For each information system, OPIC will maintain a log of all configuration changes made, the name of the person who performed the change, the date of the change, the purpose of the change, and any observations made during the course of the change.

(d) Procedures will be implemented to ensure that maintenance and repair activities are accomplished without adversely affecting system security. The procedures shall:

(1) Establish who performs maintenance and repair activities.

(2) Contain procedures for performance of emergency repair and maintenance.

(3) Contain the management of hardware/software warranties and upgrade policies to maximize use of such items to minimize costs.

(e) Version control that associates system components to the appropriate system version will be followed.

(f) Impact analyses will be conducted to determine the effect of proposed changes on existing systems and security controls.

(g) Procedures will be implemented for testing and/or approving system components (operating system, other system, utility, applications) and configuration changes prior to promotion to production.

(h) Information Users will be notified regarding how they will be impacted by changes.

(i) Current backups will be available when changes are made.

(j) All software, operating systems, and patches shall be installed in accordance with U.S. copyright regulations, the license for that software, and applicable OPIC Information Security policies.

(k) Only authorized personnel may make changes to OPIC information systems.

(l) Change control procedures will be documented for all systems to provide a complete audit trail of decisions and design modifications.

(m) Change control documentation (especially change logs) will be available even if the network is down and will not contain passwords for affected components.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that changes to the systems they own are documented and implemented in compliance with the policies and procedures listed in this document.

(b) Information Custodians are responsible for:

(1) participating in the development of procedures for change control.

(2) evaluating, recommending, and coordinating the implementation of solutions/changes consistent with OPIC technical plans.

(3) maintaining change log documentation.

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

(1) developing change control procedures.

(2) working with Information Owners and Custodians to ensure that change control policies and procedures are followed and documented.

(3) monitoring OPIC information systems to ensure compliance with this policy.

6. DEFINITIONS:

(a) Change Control - Documented procedures used to control the revision of applications, operating systems, and hardware configurations in computing environments.

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 Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(e) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(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.

BACKUP AND RECOVERY

ISSP-19-0410

1. **SUBJECT:** Backups of critical information resources must be performed, tested, and appropriately managed.
2. **SCOPE:** This policy applies to all OPIC information resources.
3. **DESCRIPTION:** There are many threats that exist which could cause the loss, corruption, or temporary unavailability of data. These include, but are not limited to, hardware failures, accidental deletion, incorrect modification, software corruption, and malicious activities. These threats are very common and it is inevitable that some of these events will occasionally occur at OPIC.

   It is therefore essential that OPIC maintain backup copies of all critical data and systems so that they can be used to provide the continued availability and viability of these resources when these events occur.
4. **PROCEDURES & GUIDELINES:**

   (a) All critical OPIC information resources will be backed up in a recoverable fashion.

   (b) Backups will be performed according to the following schedule:

   (1) All critical data and system configurations must be backed up on at least a daily basis.

   (2) Applications and licenses will be backed up whenever there are changes to them.

   (3) The backing up of non-critical data is at the discretion of the data owner.

   (c) Backups will be stored off-site in a secure, environmentally-controlled location at least 30 miles from the OPIC office.

   (d) Each system will have a defined backup retention schedule which complies with OPIC's data retention policies.

   (e) OPIC will periodically test the back up and restore procedures to ensure that data can be effectively restored from the backups.

   (f) OPIC will develop and implement detailed procedures for performing back ups restoring data, performing testing of backups, transferring tapes to/from the storage facility, and recycling or disposing of backups upon expiration of their retention period.

   (g) Backups will be treated with the same level of criticality and sensitivity as the data and applications stored on them.

   (h) Persons who have access to the backups, or who have access to perform back up or restore functions, must undergo appropriate background screening in accordance with OPIC Personnel Security policy prior to being given such access.

(i) Backup media (e.g., tapes) must be handled in accordance with OPIC Media Management policy.

(j) System custodians will back up data stored on their servers. However, information users are responsible for backing up any data stored on workstations and portable storage media (i.e., diskettes, flash drives, CDs, etc).

(1) Users may copy their data to servers to be backed up or may perform their own back ups of data not stored on OPIC servers.

(2) Backups made by users must be handled in accordance with OPIC Media Management policy.

(k) OPIC will follow NIST guidance regarding backups.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners will ensure that their resources are backed up in accordance with this policy.

(b) Information Custodians will assist Information Owners with backing up and restoring their resources.

(c) The Information Systems Security Officer (ISSO) will perform auditing to ensure compliance with this policy.

(d) Information Users will ensure that any critical data residing on their workstations or portable media are backed up in accordance with this policy.

6. DEFINITIONS:

(a) Back Up – The process of copying data to alternative or redundant media.

(b) Backup – A copy of data that is made in order to provide redundancy in case the original becomes corrupted or unavailable.

(c) Restore – The process of copying data from a previously-made backup to the original (or an alternate) system.

(d) Critical Data – Data which has been designated as “critical” under OPIC’s Information Resource Classification policy.

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) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.

(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.

PATCH MANAGEMENT AND SYSTEM UPDATES

ISSP-20-0410

1. **SUBJECT:** OPIC information systems are to be maintained with updated security patches.
2. **SCOPE:** This policy covers all servers, operating systems (OS), workstations, network devices, applications, and other information resources for which vendors provide system patches or security updates.
3. **DESCRIPTION:** Maintained patch levels are critical to the security of OPIC systems. Vendors will typically provide OS patches and fixes for security problems, which can be loaded separately from the application. These should be loaded on a regular basis using a coordinated process.
4. **PROCEDURES & GUIDELINES:**

   a) A patch management program that includes detailed procedures and standards will be developed and implemented across OPIC information resources.

   b) During regular operation, available patches will be reviewed monthly and applied if appropriate. In an emergency situation (such as an ongoing security incident), more urgent application of new security patches may be required.

   c) Patches will be checked for compatibility with all system components prior to being applied.

   d) Patches will be successfully tested on non-production systems prior to being loaded on production systems.

   e) Patching should be performed during an authorized outage window unless there is an urgent situation.

   f) Systems will be backed up prior to installation of new patches.

   g) All systems that are a part of the network infrastructure will have a log book. System log books help record the status of network equipment and provide continuity among administrators. The log book may be in paper or electronic form. Information to be recorded includes: date of the action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator remarks.

   h) In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels in effect before reloading.

   i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-40, Procedures for Handling Security Patches, and subsequent publications.
5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that their information resources are maintained in compliance with OPIC patch management policies and procedures.

(b) Information Custodians are responsible for assisting information owners with the development and implementation of patch management policies and procedures for their information resources.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing information systems to ensure that they comply with OPIC patch management policies and procedures.

6. **DEFINITIONS:**

(a) Network Device – Any physical component which forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

(b) Network Infrastructure – Network infrastructure includes servers, network devices, and any other back-office equipment.

(c) Patch – A patch is a 'fix' to a known problem with a piece of software. Instead of redistributing the entire new version of a program a patch, which is much smaller, can be applied to the old version.

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 800-40, Procedures for Handling Security Patches

(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.

SERVER SECURITY

ISSP-21-0410

1. **SUBJECT:** Servers should be made secure before placing them into the OPIC operational information technology environment, and security should be maintained throughout their lifecycle.

2. **SCOPE:** This policy applies to all OPIC information servers, including file and print servers, application servers, and database servers. All operating systems associated with these servers are also included.

3. **DESCRIPTION:** It takes only one incorrectly configured system to allow an intruder into OPIC's network. No server should ever be placed on the network without a proper security configuration.

   Additionally, as new vulnerabilities are discovered and additional security enhancements are made available, the security of the servers must continually be updated to maintain security vigilance.

4. **PROCEDURES & GUIDELINES:**

   (a) Standard base security configurations will be developed for each type of server and applied to all servers.

   (b) The level of security applied to each server will be commensurate with the level of criticality and sensitivity of the data and services that it provides.

   (c) Patch Management:

   (1) System patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures.

   (2) Logs must be kept documenting the patches and updates that have been installed on each server, including at minimum the name of the server, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.

   (d) Any unnecessary services will be disabled (*e.g.*, if a mail server does not need to allow File Transfer Protocol (FTP), then FTP should be disabled).

   (e) Access to all OPIC servers must adhere to the OPIC Access Control and Identification and Authentication policies.

   (f) Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.

   (g) All servers must run antivirus software configured in accordance with OPIC antivirus policies and procedures.

   (h) Warning banners that specify requirements and penalties for accessing the system will be provided upon access to the server.

(i) Each server must be inventoried and tracked in accordance with OPIC asset management policies and procedures.

(j) Each server's configuration must be thoroughly documented, and this documentation must be kept up to date.

(k) Any changes made to the configuration of a server must be performed in accordance with OPIC change management policies and procedures.

(l) Servers will be located in access-controlled and environmentally protected facilities, in accordance with OPIC physical and environmental security policies and procedures.

(m) Procedures will be implemented to provide verifiable backups of all servers, in accordance with OPIC data backup policie s and procedures.

(n) All servers must be assigned an Information Owner and a Custodian.

(1) These roles can be assigned to the same person or different people.

(2) Owners must be OPIC personnel. Custodians can be employees or contractors.

(o) OPIC will adhere to NIST and NSA hardening guidance for servers, as appropriate.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that any servers they own are in compliance with the guidelines provided by this policy.

(b) Information Custodians are responsible for assisting Information Owners with implementing the guidelines provided by this policy.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing servers to ensure that they are configured in accordance with the guidelines provided by this policy.

6. DEFINITIONS:

(a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.

(b) Patch – A patch is a 'fix' to a known problem with a piece of software. Instead of redistributing the entire new version of a program a patch, which is much smaller, can be applied to the old version.

(c) Server – Computer that provides a service or application that users access through a network connection.

(d) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

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) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(e) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(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.

MOBILE COMPUTING

ISSP-22-0410

1. **SUBJECT:** Laptops and other mobile computing devices require additional security controls to mitigate the risks posed by using them outside the OPIC office environment.
2. **SCOPE:** This policy applies to all laptops and other mobile computing devices that are used to store or process OPIC data.
3. **DESCRIPTION:** The use of laptop computers and mobile devices (such as PDAs) provide flexibility and enhanced communications that allow OPIC personnel to be more productive. However, the use of these devices outside of the OPIC office poses risks to those devices and the information they contain. These devices may also present a hazard to other OPIC resources upon their return to the OPIC office (for example, by spreading a virus that was obtained outside the office). These devices have the capability for direct connectivity to the Internet or other networks outside of OPICNET which lack the protections afforded by OPIC's corporate firewall and other perimeter protections. Therefore, additional security measures must be implemented to mitigate increased security risks presented by mobile computing.
4. **PROCEDURES & GUIDELINES:**

   (a) Laptops and other mobile computing devices must be inventoried and tracked.

   (b) Laptops must use antivirus and personal firewall software when connected to any network other than OPICNET.

   (c) Access to mobile devices which store or transmit sensitive data, or which can be used to connect to other sensitive OPIC systems, must be authenticated.

   (d) All security policies applied in the OPIC office environment must also be applied when using or connecting to OPIC resources outside the OPIC office environment.

   (e) Mobile computer users are responsible for backing up their data that is stored on the mobile computer on a regular basis.

   (f) OPIC sensitive data stored on laptops or other mobile devices is to be protected against unauthorized access via encryption or other appropriate measures.

   (g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.
5. **ROLES & RESPONSIBILITIES:**

   (a) Information Owners are responsible for ensuring that any mobile computing resources they own are being managed and used in accordance with the procedures and guidelines set forth in this policy.

(b) Information Custodians are responsible for assisting information owners with managing and protecting their mobile computing devices, including inventorying and tracking them, as well as defining security countermeasures that will be applied.

(c) Information Users are responsible for:

(1) Complying with the procedures and guidelines set forth in this policy.

(2) Taking all reasonable precautions to protect mobile computing devices in their possession from loss, theft, tampering, unauthorized access, and damage.

(3) Immediately reporting to the Customer Service Center the loss, theft, tampering, unauthorized access, or damage of any mobile device covered by this policy.

(d) Supervisors are responsible for ensuring that their employees understand and comply with these policies and guidelines.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of mobile computing devices to ensure compliance with the procedures and guidelines set forth in this policy.

6. DEFINITIONS:

(a) Mobile Computing Device – A laptop, PDA, or other *portable* device that can store or process data.

(b) Personal Firewall – Software installed on a computer or device which helps protect that system against unauthorized access.

(c) Antivirus Software – Software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus caused.

(d) Authentication – The process of verifying that a user is who he or she purports to be, via password, token or other credential.

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) OPIC Directive 03-01, Telecommuting Program

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

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

(e) NIST Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices

(f) 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.

NETWORK SECURITY

ISSP-23-0410

1. **SUBJECT:** Network devices and connectivity components should be made secure before placing them into the OPIC operational information technology environment, and security should be maintained throughout their lifecycle.
2. **SCOPE:** This policy applies to all routers, switches, cabling, and other network components that are part of OPIC's connectivity infrastructure.
3. **DESCRIPTION:** It takes only one incorrectly configured system to allow an intruder into OPIC's network. No network components should ever be implemented without a proper security configuration. Additionally, as new vulnerabilities are discovered and additional security enhancements made available, the configuration of the network must continually be updated to maintain security vigilance.
4. **PROCEDURES & GUIDELINES:**

(a) Standard base security configurations will be developed for each type of network component (*i.e.* routers, switches, etc.) and applied to all such components.

(b) The level of security applied to each network component should be commensurate with the level of criticality and sensitivity of the data transmitted over, and services provided by, that network.

(c) Patch Management:

(1) Patches and security updates must be applied in a timely fashion in accordance with OPIC patch management procedures.

(2) Logs must be kept documenting the patches and updates that have been installed on each device, including at minimum the name of the device, the name of the patch, the version of the patch, the date of installation, and the name of the person who installed the patch.

(d) Any unnecessary services will be disabled. (For example, if a router does not need to be managed by SNMP, then SNMP should be disabled).

(e) Access to all OPIC network devices must adhere to the OPIC Access Control and Identification and Authentication policies.

(f) Remote administration of network devices can only be performed using encrypted and authenticated connections.

(g) Auditing and logging must be enabled in accordance with OPIC auditing policies and procedures.

(h) Warning banners that specify access requirements and penalties for unauthorized access will be provided upon access to the network or device.

(i) Each device must be inventoried and tracked in accordance with OPIC asset management policies and procedures.

(j) Each device's configuration must be thoroughly documented, and this documentation must be kept up to date.

(k) Any changes made to the configuration of a device must be performed in accordance with OPIC change management policies and procedures.

(l) Network devices will be located in access-controlled and environmentally-protected facilities, in accordance with OPIC physical and environmental security policies and procedures.

(m) No device may be connected to the OPIC network without approval from the Director of Technical Services.

(n) No non-OPIC computers (e.g., contractor-owned or personal laptops) may be directly connected to the OPIC network.

(o) All network components must be assigned an owner and a custodian.

(1) These roles can be assigned to the same person or different people.

(2) Owners must be OPIC personnel. Custodians can be employees or contractors.

(p) OPIC will adhere to NIST and NSA hardening guidance for routers and other networking components, as appropriate.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any network components they own are in compliance with the guidelines provided by this policy.

(b) Information Custodians are responsible for assisting information owners with implementing the guidelines provided by this policy.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing network components to ensure that they are configured in accordance with the guidelines provided by this policy.

6. **DEFINITIONS:**

(a) Hardening – The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.

(b) Network Device – Any physical component which forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

(c) Patch – A patch is a 'fix' to a known problem with a piece of software. Instead of redistributing the entire new version of a program, a patch, which is much smaller, can be applied to the old version.

(d) Router – A device that interconnects networks and directs and filters traffic between them.

(e) Switch – A physical component that connects multiple computers and devices to a network.

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) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

    (e) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

    (f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

    (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.

PERIMETER PROTECTION

ISSP-24-0410

1. **SUBJECT:** Adequate protection must be implemented to protect OPIC information resources from intruders and service disruption.
2. **SCOPE:** This policy applies to all external entry points into OPIC information systems, including but not limited to Internet connection(s) and communication links to other agencies.
3. **DESCRIPTION:** Any connectivity to systems or organizations outside of OPIC provides an opening for unauthorized personnel to access or tamper with OPIC information resources. Such threats range from intruders breaking into OPIC's network to steal or alter data to service disruptions propagated from other systems. OPIC must implement firewalls, intrusion detection systems, and other precautions to prevent, detect, and resolve incidents arising from these threats.
4. **PROCEDURES & GUIDELINES:**

(a) OPIC will use firewalls and other security devices to provide filtering and auditing of traffic on all external communication links.

(1) OPIC will use a Firewall and an Intrusion Detection System (IDS) on all Internet connections.

(2) Routers with firewall features (e.g., packet filtering, logging) may be used for connections to other federal agencies.

(3) Traffic into OPICNET from external systems must be filtered to allow only the minimum access required to meet OPIC business requirements.

(4) Firewalls and IDS systems should be configured and administered in accordance with government and industry best practices, including but not limited to:

- The default filters must specify that all access into OPICNET be denied unless specifically permitted.
- Each firewall, IDS, and other perimeter security device must be actively monitored, and periodically audited, for threats to OPICNET.
- Firewall and IDS equipment provide real-time notifications or alerts to administrators upon security events.
- Upon a system failure, firewalls will default to a "Deny All" configuration until reset by an administrator.
- When feasible, Firewall services should run on a dedicated system with all other services disabled.
- Source routing will be disabled on all firewalls and external routers.

- The firewall will not accept traffic on its external interfaces that appears to be coming from internal network addresses.

- The firewall will be configured to implement transparency for all outbound services.

- The administrator(s) will review the network security policy and maintenance procedures on a regular basis (every three months minimum). Where requirements for network connections and services have changed, the security policy will be updated and approved.

- The firewall implementation (system software, configuration data, database files, etc.) must be backed up daily, weekly, and monthly so that in case of system failure, data and configuration files can be recovered. Backup files should be locked up so that the media is only accessible to the appropriate personnel.

- Only the firewall administrator(s) will have privileges for updating system executables or other system software. Any modification of the firewall software must be done by a firewall administrator(s) and requires the formal approval of the ISSO.

- The firewall administrator(s) must evaluate each new release of the firewall software to determine if an upgrade is required. All security patches recommended by the firewall vendor should be implemented in a timely manner.

- All services and traffic to be authorized across the firewall implementation must be well documented. Documented will be the business need, protocol used, inbound and/or outbound, port assignments, known vulnerabilities, and risk mitigation statements.

- The firewall is to run as a DNS server in order to provide public/Internet addresses to clients. The firewall will be configured to hide information about the network so that internal host data are not advertised to the outside world.

- Routing by the firewall will be disabled for a dual-homed firewall so that IP packets from one network are not directly routed from one network to the other.

(b) Any OPIC systems or services that are to be publicly available on the Internet must adhere to the following rules:

(1) These systems must be placed in a protected DMZ.

(2) No sensitive data is to be stored on systems located in the DMZ. All sensitive data must be located inside the firewall.

(3) Access from the Internet to these systems must not make sensitive information or information systems vulnerable to compromise.

(c) The details of OPIC's internal network should not be visible or accessible from outside the firewall.

(d) Proxy Servers:

(1) All outbound connections to the Internet will be performed through a Proxy server. A proxy server provides a number of security enhancements by concentrating services through a specific host to allow monitoring, hiding of internal structure, etc.

(2) Because this funneling of services creates an attractive target for a potential intruder, additional measures should be deployed to protect the proxy server.

(e) Any remote access into OPICNET through the firewall (e.g., telecommuting applications) must utilize strong authentication and encryption, and adhere to OPIC remote access policies and procedures.

(f) All perimeter equipment must be documented in accordance with OPIC information system documentation procedures.

(g) Any changes to existing equipment or deployment of new equipment on the perimeter must adhere to OPIC change control procedures.

(h) Information regarding the configuration of firewall and other perimeter protections is considered confidential and is to be treated as Sensitive But Unclassified (SBU) data.

(i) All hardware and software deployed on the perimeter must adhere to OPIC system security policies and procedures, including the disabling of all unnecessary services.

(j) All security related events on perimeter equipment, as well as access to OPICNET via this equipment, must be logged and audited in accordance with OPIC's Audit Trail policies and procedures.

(k) The responsibility for the security of any equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. COTRs are responsible for third party compliance with this policy.

(l) Employees will access the Internet only through OPIC-approved Internet access points. Any form of communication to or from workstations outside the internal (trusted) network is strictly prohibited without authorization. This includes modems, leased lines to other networks, etc.

(m) Network Trust Relationships:

(1) All connections between OPICNET and external networks (such as those of other agencies) must be approved IRM.

(2) Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures.

(3) An interconnection security agreement will be developed and signed by OPIC and the external system owner specifying security responsibilities and protections that will govern the connection between the networks.

(4) All connections to approved external networks will pass through OPIC approved firewalls.

(5) Information Owners will validate the need for all such connections on an annual basis.

(6) When notified by an Information Owner that the need for connection to a particular network is no longer valid, all accounts and parameters related to the connection should be deleted within 5 working days.

(n) The use of any of the following services on DMZ systems and perimeter systems, and the permitting of these services into OPICNET from external sources, must be approved by the ISSO: HTTP, FTP, Telnet, Finger, WHOIS, Gopher, SSL, SQL, RSH, NNTP, TN3270, Rlogin, POP3, and streaming media.

(o) Multiple layers of perimeter protections should be used to create Defense in Depth.

(p) OPIC should adhere to NIST guidance as set forth in Special Publications 800-41, Guidelines on Firewalls and Firewall Policy, 800-31, Intrusion Detection Systems; and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that the resources they own comply with the guidelines specified in this policy, including but not limited to:

(1) Obtaining appropriate authorizations and agreements for:

- Any external connections required by their systems.
- Any systems/services they own that are placed outside an OPIC firewall.
- External Access through the OPIC perimeter into their systems that are located inside OPICNET.

(2) Applying appropriate perimeter protections to any externally accessible resources that they own.

(3) Configuring any perimeter resources that they own (including security devices) in accordance with the above-specified guidance.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with the implementation and management of perimeter protections and system configurations to comply with this policy.

(2) Assisting the ISSO with auditing of perimeter protections and system configurations.

(3) Immediately reporting any perimeter breaches or potential vulnerabilities to the ISSO.

(c) Information Users are responsible for accessing the Internet and other external systems only through OPIC approved connections and in accordance with OPIC security procedures.

(d) Supervisors are responsible for ensuring that their employees understand and comply with this policy.

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

(1) Auditing OPIC information resources for compliance with this policy.

(2) Reviewing and approving access, connectivity, and services provided between OPICNET and external systems.

(3) Providing guidance to Information Owners and Custodians regarding perimeter security.

6. DEFINITIONS:

(a) DMZ (De-militarized Zone) - Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within OPICNET or to provide services to external parties.

(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) Firewall - A logical barrier guarding a private network by analyzing the data leaving and entering. It stops users or processes from going beyond a certain point in a network unless they have first passed some security test.

(d) Intrusion - Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource through unauthorized access or penetration of an information resource.

(e) Intrusion Detection System (IDS) – A system that analyzes network traffic to detect anomalies and provide alerts regarding possible intrusions.

(f) Perimeter – The boundary between OPIC owned/operated information resources and those under the control of another party.

(g) Perimeter Equipment – Any devices or servers which form part of the perimeter (e.g., perimeter router), are deployed to protect the perimeter (e.g., firewall), or which reside on the perimeter (e.g., DMZ web servers).

(h) Proxy Server - A system that acts on behalf of a user or process. Typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

(i) Strong Authentication – An authentication process using techniques which would require a high level of effort to compromise. Strong authentication usually entails the use of multiple, integrated authentication techniques (factors), such as using both a token and a PIN number together.

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 800-41, Guidelines on Firewalls and Firewall Policy.

(e) NIST Special Publication 800-31, Intrusion Detection Systems.

(f) 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.

REMOTE ACCESS

ISSP-25-0410

1. **SUBJECT:** Remote access requires additional security controls to mitigate the increased risks posed by allowing connectivity from outside the OPIC office environment.
2. **SCOPE:** This policy applies to all remote connectivity to OPIC information resources.
3. **DESCRIPTION:** Remote access to OPICNET provides many benefits. It allows personnel traveling on business to connect to OPIC information resources and provides the capability for telecommuting. However, remote access to OPIC via dial-up or other connectivity poses a risk of intrusion into OPICNET by unauthorized persons, as well as interception of the data being transferred through the remote connection. Direct connectivity to the Internet or other network outside of OPICNET also lacks the protections afforded by OPIC's corporate firewall and other perimeter protections. Additional security measures must be implemented to mitigate the increased security risks presented by remote access.
4. **PROCEDURES & GUIDELINES:**

   (a) All remote connectivity must be authenticated using strong or multi-factor authentication (such as the use of passwords in conjunction with tokens).

   (b) All sensitive data transferred over a remote access connection must be encrypted to protect it from unauthorized disclosure.

   (c) All security policies for use in the OPIC office environment must also be observed when using or connecting to OPIC resources while outside the OPIC office environment.

   (d) Any personal equipment, including personal home computers, used to connect to OPIC's information resources must meet OPIC remote access requirements, including having an approved antivirus program installed and configured with the latest updates.

   (e) OPIC sensitive data is not to be stored on any non-OPIC computers.

   (f) It is the responsibility of employees to ensure that their access devices and remote connections are not used by unauthorized persons (including family members).

   (g) Information users may not change operating system configurations, install new software, alter equipment or add to it in any way (*e.g.*, upgraded processors, expanded memory, or wireless cards), or download software from systems outside of OPIC onto OPIC remote access computers.

   (h) To prevent unauthorized users from accessing sensitive OPIC information via open modem ports, OPIC information users must log out rather than hang up after completing a remote session. They must also wait until they receive a confirmation of their log-out command from the remotely connected OPIC machine before they leave the computer they are using.

(i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-46, Security for Telecommuting and Broadband Communications, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that any remote access to their information resources is conducted in accordance with the procedures and guidelines set forth in this policy.

(b) Information Custodians are responsible for assisting information owners with implementing the guidelines outlined in this policy.

(c) Information Users are responsible for:

(1) Complying with the procedures and guidelines set forth in this policy.

(2) Protecting their remote access credentials and devices from disclosure to, or use by, unauthorized persons.

(3) Immediately reporting any suspected unauthorized use of their remote access account or any damage to or loss of OPIC computer hardware, software, or data that has been entrusted to their care.

(d) Supervisors are responsible for ensuring that their employees understand and comply with these policies and guidelines.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of remote access to ensure compliance with the procedures and guidelines set forth in this policy.

6. DEFINITIONS:

(a) Authentication - The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(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) Remote Access – Any access to OPIC's corporate network through a network, device, or medium that is not controlled by OPIC (such as the Internet, public phone line, wireless carrier, or other external connectivity).

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

(e) Strong Authentication - An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

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) OPIC Directive 03-01, Telecommuting Program

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002

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

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

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

(h) NIST Special Publication 800-46, Security for Telecommuting and Broadband Communications

(i) 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.

TELEPHONE SECURITY

ISSP-26-0410

1. **SUBJECT:** OPIC telephony resources are subject to the same security requirements and protections as other information resources.
2. **SCOPE:** This policy governs the use of telephones, modems, PBXs, and other telephony resources at OPIC.
3. **DESCRIPTION:** Telephone services are intended to support the objectives and operations of OPIC, and are critical to fulfilling OPIC's mission. These telephony resources are vulnerable to a variety of security threats and should be granted the same protection as other information resources.
4. **PROCEDURES & GUIDELINES:**

(a) When using the OPIC phone system or OPIC-issued cellular phones, users should adhere to the following guidelines to protect the information communicated:

(1) Understand that there should be no expectation of privacy when using these resources.

- OPIC may audit use of these resources.
- It is possible for third parties to tap or redirect phone calls outside of OPIC.

(2) No sensitive data should ever be discussed over a mobile phone because of the ease of intercepting such communications.

(3) Make sure that the person on the other end of the conversation is who they say they are. Do not give out sensitive information (including agency credit card information) unless you are sure of the person on the other end of the line.

(4) Be cautious when discussing sensitive information that the conversation cannot be overheard by unauthorized persons (such as visitors to OPIC). Minimize use of speakerphone.

(5) Obey relevant laws regarding the recording of phone conversations, including informing the other party that you are recording.

(6) Follow OPIC's Acceptable Use policy in using phone resources, just as you would with email or other information resources.

(b) The agency PBX and other critical telephony components must be protected:

(1) This equipment should be stored in a secure, environmentally controlled location in accordance with OPIC physical security policy.

(2) Telephony equipment is subject to the same security policies as other computer equipment, including Access Control, Change Control, Auditing, Patch Management, Server Security, Network Security, etc.

(3) Additional security threats and vulnerabilities applicable to telephony equipment must be analyzed and mitigated commensurate with the levels of risk, and criticality/sensitivity of those resources.

(c) Modems or other telephony equipment may not be installed without the explicit approval of the appropriate official (*e.g.*, OPIC Telecommunications Officer for telephone equipment, or Director of Technical Services for modems and related telephony equipment).

(d) Analog Phone Lines - As a rule, the following applies to requests for fax and analog lines:

(1) Fax lines are to be approved for departmental use only. No fax lines will be installed for personal use.

(2) Fax machines must be placed in centralized administrative areas designated for departmental use, and away from other computer equipment.

(3) A computer that is capable of making a fax connection is not to be allowed to use an analog line for this purpose.

(4) Waivers for the preceding policy on analog-as-fax lines will be delivered on a case-by-case basis after reviewing the business need with respect to the level of sensitivity and security posture of the request. If a waiver is provided, the use of an analog/ISDN fax line is conditional upon the requester's full compliance with the requirements listed below. These requirements are the responsibility of the authorized user to enforce at all times:

- The fax line is used solely as specified in the request.
- Only persons authorized to use the line have access to it.
- When not in use, the line is to be physically disconnected from the computer.
- The line will be used solely for OPIC business, and not for personal reasons.

(e) Computer-to-Analog Line Connections - The general policy is that requests for computers or other intelligent devices to be connected with analog or ISDN lines from within OPIC will not be approved for security reasons. Analog and ISDN lines represent a significant security threat to the agency, and active penetrations have been launched against such lines by hackers. Waivers to the policy will be granted on a case-by-case basis.

(1) Requesting an Analog/ISDN Line - Once approved by a manager, the individual requesting an analog/ISDN line must provide the following information to IRM:

- A clearly detailed business case of why other secure connections available at OPIC cannot be used.
- The business purpose for which the analog line is to be used.

- The software and hardware to be connected to the line and used across the line.
- The sensitivity of the data to be transferred over the line.
- To what external connections the requester is seeking access.
- Whether the machines that are using the analog lines will be physically disconnected from OPIC's internal network.
- A description of where the analog line will be placed.
- Whether dial-in from outside of OPIC will be needed.
- The number of lines being requested, and how many people will use the lines?

(2) The line must be terminated as soon as it is no longer in use.

(f) Any connectivity between the telephone system and OPICNET must be approved by the OPIC Telecommunications Officer, the Director of Technical Services, and the ISSO.

(g) OPIC will adhere to NIST guidance as set forth in Special Publication 800-24, PBX Vulnerability Analysis, and other publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for deploying, managing, and protecting their telephony resources in compliance with OPIC information security policy.

(b) Information Custodians are responsible for assisting information owners with deploying, managing, and protecting their telephony resources in compliance with OPIC information security policy.

(c) The Information Systems Security Officer (ISSO) is responsible for auditing the use and management of OPIC telephony resources to ensure compliance with OPIC information security policies.

(d) Employees are responsible for using OPIC telephony resources in an ethical, responsible, and secure manner, in accordance with this policy and existing OPIC policies.

(e) Supervisors are responsible for ensuring that their employees understand and comply with this policy.

6. DEFINITIONS:

(a) Analog - A method of transmitting information in a continuous fashion via energy waves.

(b) ISDN - A type of communication line which can carry voice, digital network services and video.

(c) Modem - A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.

(d) Private Branch Exchange (PBX) - A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.

(e) Sensitive Data/Information – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(f) Telephony - The technology associated with the electronic transmission of voice, fax, or other information between distant parties using systems historically associated with the telephone.

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) OPIC Directive 94-04, Personal Property Program Including Information Technology and Telecommunications.

(c) Federal Information Security Management Act of 2002 (FISMA), PL 107-347, December 17, 2002.

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

(e) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974.

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

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

WIRELESS SECURITY

ISSP-27-0410

1. **SUBJECT:** When using wireless networks or handheld devices, OPIC should use its risk management processes to assess the risks involved with that particular technology, to take steps to reduce those risks to an acceptable level, and to ensure that a satisfactory level of protection is maintained.

2. **SCOPE:** This policy covers all wireless data communication devices connected to OPIC networks or which are used to transmit or store OPIC data.

3. **DESCRIPTION:** Many OPIC users have found that wireless communications and devices are convenient, flexible, and easy to use. From using a handheld device to send email to using wireless connectivity in their homes, users can benefit from the increased flexibility and availability of wireless access. There may also be potential opportunities to utilize wireless LAN and WAN connectivity in the OPIC office environment.

   In addition to the risks that apply to all networks, wireless connectivity is exposed to additional vulnerabilities. Wireless networks transmit data through radio frequencies, and their transmissions may be intercepted by anyone nearby who may be listening. Unless protected, all data transmitted through a wireless connection is open to the public. Intruders have exploited this openness to access systems, destroy or steal data, and launch attacks that tie up network bandwidth and deny service to authorized users. Additionally, portable wireless devices themselves are vulnerable to loss and theft, which could lead to exposure of stored data or unauthorized access to OPIC networks via the hijacked device.

   Because of the additional risks that are faced by wireless networks and devices, additional measures need to be taken to safeguard wireless connectivity and the data that is transmitted through it.

4. **PROCEDURES & GUIDELINES:**

   (a) The use of any wireless connectivity or device for accessing or transmitting OPIC information must be approved by IRM, regardless of whether these devices are owned by OPIC.

   (b) All OPIC wireless devices must be labeled and inventoried.

   (c) Users must report any lost or stolen wireless or handheld devices to their supervisor or the OPIC ISSO as soon as possible.

   (d) Access to OPIC and other systems and networks must be immediately terminated for any lost or stolen devices.

   (e) Access to any OPIC systems or networks using wireless devices or wireless networks must be authenticated.

   (f) Security risks and controls should be evaluated more frequently for wireless technologies than for other networks and systems.

(g) Periodic security testing and assessment should be performed for any OPIC wireless networks.

(h) Ongoing, randomly timed security audits should be used to monitor and track wireless and handheld devices.

(i) Patches and security enhancements should be applied to wireless networks in accordance with OPIC system security policy.

(j) Robust cryptography must be used whenever sensitive data is stored or transmitted on a wireless device.

(k) The SSID for each device should be configured such that it does not reveal any identifying information about OPIC.

(l) Inherent security features such as authentication and encryption methods that are available in wireless technologies should be tested and used.

(m) OPIC will adhere to NIST guidance as set forth in Special Publication 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Users are responsible for:

(1) Adhering to OPIC procedures and guidelines regarding the use of wireless technologies, both within OPIC and when connecting to OPIC from remote locations.

(2) Safeguarding wireless devices in their possession.

(3) Safeguarding OPIC information resources being accessed or transmitted via any wireless technology.

(4) Promptly reporting the loss or theft of wireless devices, or any other breach of wireless security, to their supervisor or IRM.

(b) Supervisors are responsible for:

(1) Ensuring their employees understand and adhere to this policy.

(2) Forwarding reports of loss or theft of wireless devices to IRM.

(c) System Owners are responsible for:

(1) Using OPIC risk management procedures to ensure that risks have been analyzed and appropriately mitigated prior to, and during, use of any wireless technology resources that they own.

(2) Obtaining security approval prior to deploying any wireless technologies.

(3) Communicating wireless security policies and procedures to the users of their resources.

(d) System Custodians are responsible for:

(1) Safeguarding wireless information resources with which they have been entrusted.

(2) Adhering to OPIC policies and procedures for the administration of wireless devices, including:

- Labeling all wireless devices prior to deployment.
- Maintaining an inventory of all wireless devices.
- Disabling access or service for wireless devices that have been lost or stolen.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing the use of wireless technologies at, or in connection to, OPIC to ensure that appropriate security controls are used to mitigate risk.

6. DEFINITIONS:

(a) Authentication – The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(b) Cryptography – A coding method in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) using an algorithm. Cryptography is used to send or store information securely.

(c) 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.

(d) SSID – Short for **s**ervice **s**et **id**entifier, a unique identifier that acts as a password on a wireless network

(e) Wireless Technology – Any type of connectivity that transmits data without the use of physical cabling. Wireless systems include radio transmissions, satellite links, cell phones, and devices such as wireless headphones. Infrared (IR) devices such as remote controls, cordless computer keyboards, and cordless mouse devices are also included.

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 800-48, Wireless Network Security: 802.11, Bluetooth, and Handheld Devices.

(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.

SYSTEMS DEVELOPMENT

ISSP-28-0410

1. **SUBJECT:** Security must be integrated into all phases of the System Development Life Cycle (SDLC).

2. **SCOPE:** This policy covers all systems at OPIC, whether purchased or developed internally.

3. **DESCRIPTION:** Each information system passes through multiple phases during its lifetime (SDLC), as it is planned. developed, deployed, operated, and retired. Specific security-related activities must occur in each phase to assure that the system is secure.

   It is usually more cost-effective to include preventive security measures from the start rather than to deal with security breaches later on. By considering security early in the information SDLC, OPIC will be able to avoid higher costs later on while also developing a more secure system from the start.

4. **PROCEDURES & GUIDELINES:**

(a) Security must be considered in all phases of the SDLC and treated as an integral part of any system development or implementation project, including system modifications.

(b) In each phase of the SDLC there are specific information security requirements that need to be met:

(1) Initiation Phase:

- Conduct sensitivity assessment (information, potential damage, laws and regulations, threats, environmental concerns, security characteristics, OPIC policy and guidance). The assessment shall consider which laws, regulations or policies establish specific requirements for the availability, integrity, and confidentiality of the system. The environmental (e.g., hazardous location) and public threats to the system or information should also be considered.

- Perform preliminary Risk Assessment and incorporate the results into the decision-making process regarding the development/acquisition of the system.

(2) Development/Acquisition Phase:

- Security requirements shall be developed at the same time system planners define the other requirements of the system.

- The security requirements shall be incorporated into design specifications along with assurances that the security features acquired can and do work correctly and effectively. The system's security design will be documented.

- Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.
- A System Security Plan (SSP) is to be developed in accordance with OPIC System Secur ity Plan policy and procedures.
- Operational practices will be developed, including standard operational procedures and system-specific security policies (e.g., account management, backups, user training, etc.). A system handbook reflecting these practices should be developed.

(3) Implementation Phase:

- The system's security features will be configured and enabled.
- The system's security management procedures will be implemented.
- The system will be tested and authorized for processing via OPIC's Certification and Accreditation (C&A) process.

(4) Operation/Maintenance Phase:

- Perform the security activities outlined in the system security plan (e.g., performing backups, holding training classes, managing accounts.)
- Any changes made, or maintenance performed, on the system are to comply with OPIC's Change Control and Patch Management policies and processes.
- Periodic security audits and vulnerability tests will be performed in accordance with OPIC Audit and Vulnerability Testing policies.

(5) Disposal Phase:

- Information may be moved to another system, archived, discarded or destroyed in accordance with OPIC data retention policies.
- Any storage media must be disposed of in accordance with OPIC's Media Management policies.
- The disposition of software needs to be in keeping with its license or other agreements

(c) Each application must be categorized in accordance with OPIC's Information Resource Classification policy, and provided protection appropriate to its level of sensitivity and criticality.

(d) System Testing:

(1) All systems will be thoroughly tested prior to being placed in the OPIC production operating environment.

(2) Sensitive data will not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

(e) Documentation of sensitive systems must be provided the same degree of protection as that provided for the software.

(f) Application software used at OPIC must be obtained through authorized procurement channels and must comply with all licensing requirements.

(g) Systems must comply with all OPIC information security policies and procedures (e.g., system hardening, access control, backup and recovery, etc.)

(h) OPIC will adhere to NIST guidance as set forth in Special Publications 800-64, Security Considerations in the Information System Development Life Cycle, 800-12, An Introduction to Computer Security: The NIST Handbook, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for:

(1) Understanding the security requirements for each system life cycle phase.

(2) Implementing the life cycle security requirements for their systems.

(3) Documenting the security controls in the System Security Plan.

(4) Ensuring that security controls are incorporated in the design, development, and testing of contractor-developed software.

(5) Accrediting systems in accordance with OPIC C&A policy.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with the development and implementation of security controls.

(2) Ensuring that system security controls are implemented properly and operating as intended.

(3) Maintaining the system in accordance with all standard operating procedures and other approved security management processes.

(4) Assisting the ISSO with testing and auditing of the system.

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

(1) Assisting System Owners in addressing the security issues present in each life cycle phase.

(2) Providing baseline security requirements to be used for OPIC systems.

(3) Auditing to ensure that all systems are in compliance with this policy.

(4) Performing certification of systems in accordance with OPIC C&A policy.

6. DEFINITIONS:

(a) Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.

(b) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(c) System Development Life Cycle – The system development life cycle (SDLC) starts with the initiation of the system planning process, and continues through system acquisition/development, implementation, operations and maintenance, and ends with disposition of the system.

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

7. **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) Office of Management and Budget (OMB) Circular No. A-130, "Management of Federal Information Resources."

(d) Office of Management and Budget Memorandum M-00-07, "Incorporating and Funding Security in Information Systems Investments," February 28, 2000.

(e) Computer Security Act of 1987, P.L. 100-235 (1988).

(f) Federal Information Processing Standards (FIPS) Publication 73, Guidelines for Security of Computer Applications, June 1980.

(g) NIST Special Publication 800-64, Security Considerations in the Information System Development Life Cycle.

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

(i) NIST Special Publication 800-12, An Introduction to Computer Security: The NIST Handbook.

(j) NIST Special Publication 500-153, Guide to Auditing for Controls and Security: A System Development Life Cycle Approach.

10. **LOCATION:** TBD

11. **EFFECTIVE DATE:** October 22, 2004

12. **REVISION HISTORY:** None

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

ELECTRONIC MAIL

ISSP-29-0410

1. **SUBJECT:** Electronic mail must be protected from the threats and vulnerabilities that can cause system damage, data compromise, and business disruption.
2. **SCOPE:** This policy applies to the use of any OPIC information resource to transmit, receive or store electronic mail, as well as use of any non-OPIC email systems to transfer OPIC data.
3. **DESCRIPTION:** Electronic mail is an essential tool used by OPIC to conduct its business. Email is a vital method of exchanging messages and data files over computer networks.

   However, email is inherently insecure and presents many risks to OPIC information security. Email can be read, altered, or deleted by unknown parties without the permission of the person who sent or received the message. Email can also be used to distribute viruses and other harmful code that pose a threat to OPIC resources. Information users might also send inappropriate, proprietary, or other sensitive information via email, thus exposing OPIC to legal action or damage to its reputation. After web servers, an organization's mail servers are typically the most frequent targets of attack. Therefore, it is crucial to take prudent security precautions in administering and using email.
4. **PROCEDURES & GUIDELINES:**

   (a) Information Users must understand that email can be intercepted or altered without the knowledge of the sender or recipient when it is transferred over the Internet.

   (b) Sensitive information may not be sent over the Internet (via email or other means) without being encrypted. Sensitive information should be encrypted when transferred outside of OPICNET.

   (c) To ensure data is adequately protected, OPIC personnel may only send OPIC data via OPIC owned or operated email systems.

   (1) Permission may be granted by Management to use an alternate system in the case of an emergency.

   (2) OPIC information users are not permitted to forward OPIC email or attachments to personal accounts managed by public email or Internet service providers where the information might be compromised.

   (d) Information users are prohibited from using any OPIC email systems (or any other email systems accessed from OPIC computers) for prohibited purposes, as outlined in OPIC's Acceptable Use of Information Resources policy and Management Directive 94-04.

   (e) Information users may not direct unauthorized or personal messages to the All OPIC distribution group or other large groups of users.

(f) Emails should be deleted once no longer needed. Old emails that must be retained should be archived from the email server on a periodic basis.

(g) The following procedures should be used to avoid potential damage caused by email-borne computer viruses:

(1) All incoming emails should be scanned for viruses in accordance with the OPIC Antivirus policy.

(2) Information users should not open attachments or click on links in messages from senders they do not know.

(3) Information users should report all suspicious emails to the ISSO or the CSC.

(4) Emails containing executable attachments should be filtered and quarantined from entering the OPIC network.

(h) To minimize spam and avoid waste of OPIC resources, information users must avoid using their OPIC email addresses for personal correspondence on the Internet, particularly if they do not know or have a trust relationship with the other party. This especially includes giving out one's official email address to Internet shopping sites, bulletin boards, and mailing lists.

(i) Information users shall have no expectation of privacy while using OPIC's email system.

(j) OPIC will adhere to NIST guidance as set forth in Special Publication 800-45, Guidelines on Electronic Mail Security, and subsequent publications.

5. **ROLES & RESPONSIBILITIES:**

(a) Information Owners are responsible for ensuring that any email system they own, and the data they own which is transmitted via email, adhere to this policy and its associated procedures and guidelines.

(b) Information Custodians are responsible for assisting information owners in implementing the procedures and guidelines specified in this document.

(c) Information Users are responsible for adhering to the procedures and guidelines provided in this document.

(d) Supervisors are responsible for ensuring that their employees understand and adhere to the procedures and guidelines provided in this document.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing email systems and usage to ensure compliance with the procedures and guidelines provided in this document.

6. **DEFINITIONS:**

(a) Information Resources - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information.

(b) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(c) Spam – Unauthorized and unsolicited electronic mass mailings.

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) 5 U.S.C. 552A, Records Maintained on Individuals and The Privacy Act of 1974, as amended

(e) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

(f) NIST Special Publication 800-45, Guidelines on Electronic Mail Security.

11. **LOCATION:** TBD

12. **EFFECTIVE DATE:** October 22, 2004

13. **REVISION HISTORY:** None

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

DATABASE SECURITY

ISSP-30-0410

1. **SUBJECT:** Securing information, so that it remains consistent, complete, and accurate, is essential to OPIC's reputation, mission, and critical business objectives.
2. **SCOPE:** This policy applies to all OPIC databases.
3. **DESCRIPTION:** OPIC has been entrusted with a variety of sensitive data to accomplish its goals. The success of agency programs depends on the availability, integrity and confidentiality of this data. In order to protect this data, OPIC must implement data security measures, such as data validation and verification controls. These controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets the expectations about its quality and that it has not been altered.
4. **PROCEDURES & GUIDELINES:**

(a) Data will be secured commensurate with its level of sensitivity and criticality.

(b) Databases, and applications that interface with databases, will be configured in accordance with security best practices:

(1) Integrity verification programs, such as consistency and reasonableness checks, shall be used to look for evidence of data tampering, errors, and omissions.

(2) Reconciliation routines (checksums, hash totals, record counts) shall be used to ensure software and data have not been modified.

(3) If users are allowed to make updates to a database via a web page, these updates should be validated to ensure that they are warranted and safe.

(4) For databases containing sensitive information, table access controls should be applied. Access to specific information within the database should be limited to only those personnel who need access to that information, and access should be limited to only those functions (e.g., read, write, modify, etc.) required for the person to perform his or her duties.

(5) Database servers should be configured to only allow connections from authorized, trusted sources (such as the specific web servers to which they supply information).

(6) For sensitive data, audit trails should be created and maintained within the database to track transactions and provide accountability.

(7) Securing sensitive information by selectively encrypting data within the database is encouraged.

(c) Programs or utilities that may be used to maintain and/or modify sensitive databases and other software modules that could affect or compromise the confidentiality, integrity, or availability of the data, must be carefully controlled.

(d) Databases containing non-public information should never be on the same physical machine as a web server.

(e) Databases (and database servers) that store public information cannot be used to also store non-public (e.g., private, proprietary, sensitive) information.

(f) Integrity errors and unauthorized or inappropriate duplications, omissions, and intentional alterations will be reported to the Information Owner.

(g) Database servers and database software must adhere to all OPIC information security policies and procedures pertaining to servers and systems, including patching, hardening, change control, authentication, etc.

(h) OPIC will follow NIST guidance regarding database security.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for the following for data that they own:

(1) Ensuring the confidentiality, integrity, and availability of the data.

(2) Ensuring that data integrity and validation controls are installed, operated and maintained.

(3) Authorizing and limiting access to data they own.

(4) Reporting database security incidents to the ISSO.

(b) Information Custodians are responsible for:

(1) Assisting Information Owners with maintaining the confidentiality, integrity, and availability of their data.

(2) Assisting Information Owners with implementing the prescribed database security controls.

(3) Immediately reporting breaches of database security to the Information Owner and the ISSO.

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

(1) Providing guidance to Information Owners and Custodians regarding database security.

(2) Auditing OPIC databases, servers, and applications to ensure compliance with this policy.

(d) Information Users are responsible for:

(1) Not accessing data that they are not authorized to access and/or for which they do not have a legitimate business need to know.

(2) Exercising due diligence to prevent accidental misentry, modification or deletion of data.

(3) Immediately reporting any security incidents to the Information Owner or Custodian.

(e) Supervisors are responsible for:

(1) Ensuring that their employees understand and comply with this policy.

(2) Reporting any suspected incidents to the ISSO and the Information Owner.

6. DEFINITIONS:

(a) Availability - Assuring information and communications services will be ready for use when expected

(b) Confidentiality - Assuring information will be kept secret, with access limited to appropriate persons.

(c) Data - A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

(d) Database - An organized collection of logically related information stored together in one or more computerized files.

(e) Integrity - Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete, and consistent.

(f) Sensitive Data – Any data that is categorized as "sensitive" under OPIC's information resource classification policy and framework.

(g) Validation - The checking of data for correctness and/or for compliance with applicable standards, rules, and conventions.

(h) Verification - The process of ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.

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 800-12, "An Introduction to Computer Security: The NIST Handbook." October 1995.

(e) NIST Special Publication 800-53, Recommended Security Controls for Federal Information 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.

MEDIA MANAGEMENT

ISSP-31-0410

1. **SUBJECT:** Media must be handled, stored, and disposed of properly in order to protect the sensitive or critical OPIC data stored upon it.
2. **SCOPE:** This policy applies to all media that is used to store OPIC data.
3. **DESCRIPTION:** OPIC has been entrusted with a variety of sensitive data in order to accomplish its mission. This data, which is stored on a variety of media, must be protected from unauthorized disclosure, damage, fraud, and abuse. To protect the security and privacy of information, OPIC will use a variety of security mechanisms that provide protections for media.
4. **PROCEDURES & GUIDELINES:**

(a) Media Handling:

(1) Users should take all reasonable steps to protect OPIC storage media in their possession from tampering or accidental damage.

(2) Users are responsible for making their own backups of any data that is not stored on OPIC servers.

(3) Appropriate physical and environmental protection controls shall be provided for stored media.

(4) Handling media that contain sensitive data:

- Any media containing sensitive data should be marked with its classification level. Labeling shall include any special handling instructions
- Any media containing sensitive data must be secured (such as kept in a locked drawer, cabinet, or safe) when not in use or unattended. Any media sensitive information transported through the mail or courier/messenger service shall be double-sealed, the second envelope shall be appropriately marked with the sensitivity classification of the data.
- The receipt and delivery of media containing sensitive data must be monitored and accounted for to ensure that data is not lost and potentially compromised while in transit.
- Sensitive information shall be turned over or shall be put out of sight when visitors are present.

(b) Media Disposal:

(1) Information Users need to understand that simply deleting data from media does not completely or permanently remove the information. Deleted files are susceptible to unauthorized retrieval if not disposed of properly.

(2) Media that contain sensitive data must be sanitized when they are no longer needed to store the sensitive data.

(3) Before any OPIC-owned or managed computing equipment is transferred, donated, or otherwise disposed of, storage media associated with the equipment must be sanitized via approved government methods.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for ensuring that any media they own, and media that contains data or applications that they own, are handled and disposed of in accordance with OPIC policies and procedures.

(b) Information Custodians are responsible for:

(1) Assisting information owners with the proper handling of their media in accordance with OPIC policies and procedures.

(2) Complying with OPIC policies and procedures for any media entrusted to them.

(3) Reporting the loss, damage, or theft of any media entrusted to them that contains OPIC data.

(c) Information Users are responsible for:

(1) Protecting OPIC media in their possession from tampering or accidental damage.

(2) Storing OPIC data only on approved media.

(3) Backing up data that is stored on media in their physical possession.

(4) Reporting the loss, damage, or theft of any media containing OPIC data.

(d) Supervisors are responsible for:

(1) Ensuring that their employees understand how to properly handle and dispose of media in accordance with OPIC policies and procedures.

(2) Communicating changes in policies and procedures to their staff.

(e) The Information Systems Security Officer (ISSO) is responsible for developing media management standards and performing auditing to ensure that media is being handled and disposed of in accordance with OPIC policies and procedures.

6. DEFINITIONS:

(a) Media – Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.

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

(c) Sanitization - To expunge data from storage media so that data recovery is impossible. The most common types of sanitization are destruction (*e.g.* burning or smashing), degaussing (*i.e.* demagnetizing), and overwriting.

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) The Privacy Act of 1974, as amended, PL 93-579, December 31, 1974

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

(f) Homeland Security Presidential Directive / HSPD-7, December 17, 2003

(g) Computer Abuse Amendments Act of 1994, PL 103-322, September 13, 1994

(h) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers

11. **LOCATION:** TBD

12. **EFFECTIVE DATE:** October 22, 2004

13. **REVISION HISTORY:** None

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

PASSWORD MANAGEMENT

ISSP-32-0410

1. **SUBJECT:** OPIC will protect access to its information resources by ensuring that any passwords used for authentication are properly assigned and protected.

2. **SCOPE:** This policy applies to all OPIC owned or operated information systems, both operational and in development.

3. **DESCRIPTION:** In order for passwords to be an effective tool for providing security, they must be selected, stored, and administered appropriately. If passwords are poorly chosen, they can easily be guessed and then used by unauthorized persons. Likewise, passwords that are inappropriately stored are subject to disclosure and misuse by unauthorized persons.

4. **PROCEDURES & GUIDELINES:**

(a) In systems that use passwords as their authentication method, every account (including newly issued accounts) will have a password.

(b) Passwords must be changed:

(1) Immediately upon initial user logon.

(2) At least every 90 days.

- Individual systems may set a shorter expiration period for their users.
- Systems will have an automated mechanism to ensure that passwords are changed.

(3) If it is suspected that the password has been compromised.

(4) For administrator accounts, immediately upon the departure of personnel with access to those accounts, or upon suspected compromise of those passwords.

(c) The following guidelines apply to password storage and visibility:

(1) Passwords will not be visible on a screen, hardcopy or other output device.

(2) Passwords will never be stored in a clear text file. This includes storage of passwords in configuration files, database files, application code, and system directories. Any such passwords must be encrypted if they are required.

(3) Passwords will not be sent via unsecured (i.e., unencrypted and unauthenticated) email.

(4) Passwords will not be stored in written form (*e.g.* sticky notes) except if secured in an approved locked area.

(d) Passwords are never to be lent or divulged to other persons, including individuals purporting to be system administrators.

(e) A poorly chosen password could compromise the entire OPIC computer network. The object when choosing a password is to make it as difficult as possible for someone to guess what you have chosen. The following guidelines should be used to select strong, effective passwords:

(1) Users with multiple accounts on the same OPIC system (*e.g.* an administrative account and a regular user account) must use completely different passwords for each account. Generic or group passwords will not be used.

(2) Users are not to use the same password at OPIC that they use for any non-OPIC computer accounts (*e.g.* an account on an Internet website).

(3) Passwords should be at least 8 characters and contain a combination of letters, numbers, and special characters.

(4) Passwords cannot be reused for at least four changes.

(5) Never assign a login account a password that is the same string as the User ID or that contains the User ID (*e.g.,* "bob123" is not an appropriate password for user "bob").

(6) Never set any password equal to the null string (*i.e.,* a blank password), which is equivalent to no password at all.

(7) Passwords should not be a dictionary word in any language.

(8) Passwords should not contain any proper noun or the name of any person, pet, child, or fictional character.

(9) Passwords shall not contain any employee serial number, Social Security Number, birth date, telephone number, or any information that could be readily guessed about the creator of the password.

(10) Passwords should not contain any simple pattern of letters or numbers, such as "xyz123."

(11) Passwords should not share more than 3 sequential characters in common with a previous password (*i.e.,* do not simply increment the number on the same password, such as fido1, fido2, etc.).

(12) Use a password that is easy to remember (*e.g.,* a phrase, line from a song, or nonsense words) and that you can type quickly.

(f) The assignment of passwords for specific OPIC systems should adhere to the following:

(1) Each system should have its own password selection standard that adheres to the above guidelines while being commensurate with the level of security required by the level of sensitivity of the system.

(2) The system will be configured to enforce the password selection criteria specified in the system criteria.

(g) Users should avoid using the "remember password" feature on web sites and other applications.

(h) If SNMP is used, the community strings should follow the same selection guidance provided for passwords.

(i) OPIC will adhere to NIST guidance as set forth in Special Publication 800-63, Recommendations for Electronic Authentication, and subsequent publications.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners shall ensure that the resources they own comply with the guidelines set forth in this policy.

(b) Information Custodians shall:

(1) Assist Information Owners with implementing measures to enforce policy selection and management on their systems.

(2) Instruct users regarding system password policy.

(3) Assist the ISSO with auditing for compliance with this policy.

(4) Report any password compromises of OPIC information resources to the ISSO and the Information Owner.

(c) Employees shall understand their responsibilities for selecting and safeguarding their passwords, and immediately notify a supervisor or the Information Custodian if they suspect that a password has been compromised.

(d) Supervisors shall:

(1) Ensure that their personnel understand and comply with the guidelines contained in this policy.

(2) Report any suspected violations or password compromises to the ISSO and the Information Custodian.

(e) The Information Systems Security Officer (ISSO) shall:

(1) Provide advice to Information Owners and Custodians regarding system-specific password policies.

(2) Audit systems to ensure compliance with this policy

(f) System Developers must ensure that their systems support the procedures and guidelines specified in this policy document.

6. DEFINITIONS:

(a) Authentication – The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that is part of the user, such as a fingerprint or iris.

(b) Password – Any secret string of characters which serves as authentication of a person's identity, and which may be used to grant or deny access.

(c) User ID - Character string that uniquely identifies a computer user or computer process.

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) 18 U.S.C. 1030, Fraud and Related Activities in Connection with Computers.

    (d) Homeland Security Presidential Directive / HSPD-7, December 17, 2003.

    (e) NIST Special Publication 800-63, Recommendations for Electronic Authentication.

    (f) 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.

ASSET MANAGEMENT

ISSP-33-0410

1. **SUBJECT:** All information assets must be tracked and managed to ensure that they are not lost or misused.

2. **SCOPE:** This policy applies to all OPIC information assets, including but not limited to workstations, servers, network devices, printers, personal digital assistants (PDAs), phones, software, and licenses.

3. **DESCRIPTION:** Each year, thousands of information assets are lost or stolen. Often agencies simply lose track of these items, sometimes resulting in scandals that appear in the news, and at minimum incurring the wrath of auditing organizations like GAO and OMB.

   Not only would loss of information assets result in a financial impact on OPIC, but it could also result in unauthorized access to data stored on or accessed through these assets, and could have a detrimental effect on the reputation of the agency. Additionally, the tracking and management of information assets is mandated by several federal regulations, such as the Clinger-Cohen Act.

4. **PROCEDURES & GUIDELINES:**

   (a) OPIC must keep a record of all information assets, including those mentioned in the scope above.

   (1) Information assets are to be added to the record upon receipt by OPIC and assigned a barcode.

   (2) For each information asset, OPIC will track at least the following information:

   - The brand, model, and type of asset
   - Serial number and OPIC barcode
   - The person to whom the asset is assigned
   - The location of the asset
   - Any maintenance agreements for the asset
   - The date of receipt of the item
   - Date the record was last updated or inventoried

   (3) Upon disposal of an information asset, OPIC will track the date of disposal, the method of disposal (e.g., transfer, destruction, donation, etc.), and the name of the new owner (if there is one).

   (b) Periodic inventories are to be performed to verify records and account for all information assets.

   (1) Each asset is to be inventoried at least annually.

5. ROLES & RESPONSIBILITIES:

(a) Information Owners are responsible for inventorying, tracking, and protecting the OPIC information resources that they own.

(b) Information Custodians are responsible for assisting information owners with inventorying, tracking, and protecting OPIC information resources in their care.

(c) Information Users are responsible for exercising due diligence in protecting information resources entrusted to them, and immediately reporting the loss, theft or damage of any OPIC information resource.

(d) Supervisors are responsible for ensuring their employees understand their responsibilities regarding protection of information resources.

(e) The Information Systems Security Officer (ISSO) is responsible for auditing to ensure that information assets are being tracked and managed in accordance with this policy.

6. DEFINITIONS:

(a) Information Asset – An information resource that has tangible value.

(b) Information Resource - The procedures, equipment, facilities, software and data that are designed, built, operated and maintained to collect, record, process, store, retrieve, display and transmit information

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

(e) Federal Managers Financial Integrity Act of 1982 PL 97-255 (H.R. 1526).

11. LOCATION: TBD

12. EFFECTIVE DATE: October 22, 2004

13. REVISION HISTORY: None

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

APPENDIX C: INFORMATION SECURITY GLOSSARY

Glossary of Security Terms

Access — 1. The right to enter or make use of a computer system 2. To approach, view, instruct, communicate with, store data in, retrieve data from, or otherwise make use of computers or information resources.

Access Control — The enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Access Control List — List that contains a set of access control entries that define an object\'s permission settings and enables administrators to explicitly control access to resources.

Account — A set of privileges for authorization to system access, which are associated with a userid.

Accountability — The responsibilities and accountability of owners, providers and users of information systems and other parties...should be explicit.

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.

Active Attack — An attack which results in an unauthorized state change, such as the manipulation of files, or the adding of unauthorized files.

Administrative Security — The management constraints and supplemental controls established to provide an acceptable level of protection for data

Alert — A formatted message describing a circumstance relevant to network security. Alerts are often derived from critical audit events.

Algorithm — A mathematical process for performing a certain calculation; in the information security field, generally used to describe an encryption process.

Analog — A method of transmitting information in a continuous fashion via energy waves.

Anti-virus Software — Commercially available software that searches for evidence of computer virus infection and attempts to remove the malicious code and repair any damage the virus may have caused.

Archival Data — Information no longer in use, but which must be retained, and is stored separately to free space on a drive.

Assessment — Surveys and Inspections; an analysis of the vulnerabilities of a system. Information acquisition and review process designed to assist a customer to determine how best to use resources to protect information in systems.

Assurance — A measure of confidence that the security features and architecture of a system accurately mediate and enforce the security policy.

Attack — An attempt to bypass security controls on a computer.

Audit Trail — In computer security systems, a chronological record of system resource usage. This includes user login, file access, other various activities, and whether any actual or attempted security violations occurred, legitimate and unauthorized.

Authentication — The process of verifying that a user is who he or she purports to be. Techniques are usually broken down into three categories: (1) something the user knows, such as a password or

PIN; (2) something the user has, such as a smartcard or ATM card; and (3) something that\'s part of the user, such as a fingerprint or iris.

Authentication Token A hardware device, the possession of which can be verified, and which helps to confirm identity as part of the authentication process (*e.g.*, smartcard, SecureID)

Authorization The process of granting privileges to an authenticated user or entity.

Authorized Telework Approved work performed by an employee away from his or her duty station that requires connectivity to OPIC information resources.

Automated Information System Any equipment of an interconnected system or subsystems of equipment that is used in the automatic acquisition, storage, manipulation, control, display, transmission, or reception of data and includes software, firmware, and hardware

Availability Assuring information and communications services will be ready for use when expected.

Awareness A state of focused attention on security that allows individuals to recognize IT security concerns and respond accordingly.

Back Door Secret (undocumented), hard-coded access codes or procedures for accessing information.

Back Up The action of copying (or mirroring) important data to a second location or onto removable media

Backbone High-speed line or series of connections that forms a major pathway within a network.

Bandwidth Speed at which information can be transferred.

Biometric Scanner A device connected to a computer system that recognizes physical characteristics of an individual (e.g., fingerprint, voice, retina).

Biometrics The identification of a user based on a physical characteristic, such as a fingerprint, iris, face, voice or handwriting.

BIOS (Basic Input Output System) The set of routines stored in read-only memory that enable a computer to start the operating system and to communicate with the various devices in the system such as disk drives, keyboard, monitor, printer, and communication ports. The BIOS also stores the date, time and configuration of the hardware.

Breach The successful defeat of security controls which could result in a penetration of the system. A violation of controls of a particular information system such that information assets or system components are unduly exposed.

Brute Force Attack Attack where the attacker attempts to “guess” a password or other secret by trying all possible values.

Buffer An area of memory used for temporary storage of data read from or waiting to be sent to a device.

Buffer Overflow Situation where more data is put into a buffer or holding area than the buffer can handle.

Bug An unwanted and unintended property of a program or piece of hardware, especially one that causes it to malfunction.

Building Service Contractors Includes, but is not limited to, custodians, mechanics, electricians, plumbers, and guards.

Business Need-to-Know A security concept that limits access only to information and information processing resources required for performing one’s normal business related duties.

Certification An assessment of the security controls of an information system.

CGI Scripts Programs that allow for the creation of dynamic and interactive web pages.

Chain of Custody Verifies that information was not altered in the copying process and has not been altered during any analysis.

Challenge/Response Password A one-time password generating device, token, or SmartCard used in place of a reusable password.

Change Management Change management is documented procedures used to control the revision of applications and or operating systems in computing environments.

Circuit Level Gateway One form of a firewall. Validates TCP and UDP sessions before opening a connection. Creates a handshake, and once that takes place passes everything through until the session is ended.

Client Software that resides on the user's computer and communicates with a server(s).

Cluster Groupings of sectors that are used to allocate the data storage area.

Common Gateway Interface (CGI) The method that Web servers use to allow interaction between servers and programs.

Compliance Statement A document used to obtain a promise from a computer user that the user will abide by system policies and procedures.

Compromise An intrusion into a computer system where unauthorized disclosure, modification or destruction of sensitive information may have occurred.

Computer Abuse The willful or negligent unauthorized activity that affects the availability, confidentiality, or integrity of computer resources. Computer abuse includes fraud, embezzlement, theft, malicious damage, unauthorized use, denial of service, and misappropriation.

Computer Forensics The act of looking for and preserving digital evidence of a crime for eventual use in court.

Computer Fraud Computer-related crimes involving deliberate misrepresentation or alteration of data in order to obtain something of value.

Computer Network Attack Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

Computer Security The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Computer-Created Files Files such as backup files, configuration files, cookies, hidden files, history files, log files, printer spool files, swap files, system files, temporary files.

Confidential Information A classification for information whose disclosure may damage OPIC, the federal government, our customers, or other parties.

Confidentiality 1. A requirement that private or confidential information not be disclosed to unauthorized individuals. 2. Assuring information will be kept secret, with access limited to appropriate persons.

Containment The phase in Incident Handling that limits the scope and magnitude of an incident Information given to you when you log into or otherwise access a system.

Contingency Plan Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

Continuity Of Operations Plan (COOP) A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained for up to 30 days as a result of a disaster event before returning to normal operations.

Continuity of Support Plan (COSP) The documentation of a predetermined set of instructions or procedures mandated by Office of Management and Budget (OMB) A-130 that describe how to sustain major applications and general support systems in the event of a significant disruption.

Contract Any U.S. Government contract or agreement issued or made by or on behalf of OPIC

Contractor. Any non-Federal employees working on any U.S. Government contract

Control Statement A statement that applies to information which informs the user of special requirements, restrictions or protection.

Cookie Small file on your computer in which a web site may write data.

Countermeasures Action, device, procedure, technique, or other measure that reduces the vulnerability of an automated information system.

Cracker A malicious, criminal hacker who uses tools to decode encrypted passwords to break into a computer system and makes an unauthorized penetration of computer systems and networks, abuse of privileges, or unauthorized use of services.

Crash A sudden, usually drastic failure of a computer system.

Critical Information Any information essential to OPIC's activities, the destruction, modification, or unavailability of which would cause serious disruption to the agency's mission.

Critical Infrastructure A foundation of services that citizens and businesses rely on for their health, safety and well-being. Telecommunications, transportation, energy and banking services are part of the critical infrastructure, which is often privately owned but which citizens expect the government to protect.

Cryptanalysis 1) The analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including cleartext. Definition 2) Operations performed in converting encrypted messages to plain text without initial knowledge of the crypto-algorithm and/or key employed in the encryption.

Cryptography A coding method in which data is encrypted (translated into an unreadable format) and then decrypted (translated back into a readable format by someone with a secret key) using an algorithm. Cryptography is used to send or store information securely.

Cyberspace Describes the world of connected computers and the society that gathers around them. Commonly known as the INTERNET.

Data A representation of facts or concepts in an organized manner in order that it may be stored, communicated, interpreted, or processed by automated means.

Data Diddling Modifying data for fun and profit; e.g., modifying grades, changing credit ratings, altering security clearance information, fixing salaries, or circumventing bookkeeping and audit regulations.

Data Driven Attack A form of attack that is encoded in innocuous seeming data which is executed by a user or a process to implement an attack.

Data Encryption Standard A cryptographic algorithm for the protection of unclassified data, published in Federal Information Processing Standard (FIPS) 46. The DES, which was approved by the National Institute of Standards and Technology (NIST), is intended for public and government use.

Data integrity The requirement that information and programs are changed only in a specified and authorized manner."[1]

Data Leakage Uncontrolled, unauthorized transmission of classified information from a data center or computer system to the outside. Such leakage can be accomplished by physical removal of data storage devices (diskettes, tapes, listings, printouts and photographs of screen copies or handwritten notes) or by more subtle means such as data hiding (steganography) or even human memory.

Data Mapping Going beyond basic search capabilities, data mapping is also called keyless searching. It finds or suggests associations between files within a large body of data, which may not be apparent using other techniques.

Database An organized collection of logically related information stored together in one or more computerized files.

Decryption The mathematical process by which an encrypted message is rendered readable or usable (reverses the encryption process).

Degaussing Degaussing (i.e., demagnetizing) is a procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.

Denial-of-Service Attack (DoS) An attack in which a network, server, or even a telephone system is purposely overloaded with phony requests so that it cannot respond properly to valid ones. Prevents normal use of computer or network by valid users where the attacker can cause abnormal termination of the applications, flood the network with traffic, or block traffic.

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.

Dial-in The capability to allow one system to access information or receive a message from another system over non-dedicated public phone lines.

Dial-in Modem A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator

[1] National Research Council, *Computers at Risk*, (Washington, DC: National Academy Press, 1991), p. 54.

Digital Data that has been created, transmitted, or stored as a string of signals coded as "1" (on) or "0" (off). Data in digital form (text, numbers, graphics, voice, video, etc.) can be stored and processed by computers and communicated at high speed over electronic networks with complete accuracy and reliability.

Digital Certificate The electronic equivalent of an ID card, which works in conjunction with public key encryption to sign digital signatures. 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.

Digital Evidence Information stored or transmitted in binary form that may be relied upon in court.

Digital Signature A sequence of bits which accompanies a message that is generated via encryption; such a bit sequence shows that a message (a) was sent by an identified person, and (b) is free from modification or tampering.

Digital Subscriber Line (DSL) A form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).

Disaster A condition in which an information resource is unavailable, as a result of a natural or manmade occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of agency program objectives, as determined by agency management.

Disaster Recovery Written plan describing the steps company would take to restore computer operations in the event of a disaster

Disaster Recovery Plan (DRP) A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

Disclosure Unauthorized access to confidential or sensitive information.

Disruption An unplanned event that causes the system to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

Distributed Denial-of-Service Attack (DDoS) A denial-of-service attack in which the attackers load their malignant code onto a host of other machines (often through Trojan horses). Distributed attacks can cause much more damage than an attack originating from a single machine, as the defending company needs to block dozens or even hundreds of IP addresses. Compromised hosts used to attack other Internet sites, altering system binaries, and exposing sensitive information to external parties.

DMZ (de-militarized zone) Any un-trusted network connected to, but separated from, the corporate network by a firewall, used for external (Internet/partner, etc.) access from within <Company Name>, or to provide information to external parties.

DNS Spoofing Assuming the DNS name of another system by either corrupting the name service cache of a victim system, or by compromising a domain name server for a valid domain.

Dongle A small device that plugs into a computer port that contains types of information similar to information on a smart card. Also called a hardware key.

Dual Homing Having concurrent connectivity to more than one network from a computer or network device.

Dynamic password A password which changes each time a user logs-into a computer system (typically accomplished via smart cards).

E-commerce Transactions where money is exchanged for valuable goods and services with either the money and/or the goods and services transported over computer networks.

Electronic Evidence Information and data of investigative value that is stored on or transmitted by an electronic device. Such evidence is acquired when data or physical items are collected and stored for examination purposes.

Emergency Disk Floppy disk that contains an unaffected copy of operating system.

Employee Non-work Time Times when the employee is not otherwise expected to be addressing official business.

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, especially during transmission

Encryption key A secret password or bit string used to control the encryption process.

End User An individual who employs computers to support OPIC activities, who is acting as the source or destination of information flowing through a computer system.

Eradication The phase in Incident Handling that makes sure the problem is eliminated and the avenue of entry is closed off Information given to you when you log into or otherwise access a system.

Exposure The condition of vulnerability to loss resulting from accidental or intentional disclosure, modification, or destruction of information resources.

False Negative Occurs when an actual intrusive action has occurred but the system allows it to pass as non-intrusive behavior.

False Positive Occurs when the system classifies an action as anomalous (a possible intrusion) when it is a legitimate action.

Fault Tolerance The ability of a system or component to continue normal operation despite the presence of hardware or software faults.

Field A single piece of information stored in a database.

Firewall A logical barrier guarding a private network by analyzing the data leaving and entering. It stops users or processes from going beyond a certain point in a network unless they have first passed some security test.

Follow-Up The phase in Incident Handling that identifies lessons learned, improves incident handling capability, and tabulates finding in a report format Information given to you when you log into or otherwise access a system.

Gateway Enables two technologically different networks to communicate.

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.

Government Office Equipment Includes but is not limited to: personal computers and related peripheral equipment and software, library resources, telephones to include cellular, facsimile machines, photocopiers, office supplies, Internet connectivity and access to Internet services, and E-mail

Hacker A person who enjoys exploring the details of computers and how to stretch their capabilities. A malicious or inquisitive meddler who tries to discover information by poking around.

Hacking Run A hack session extended long outside normal working times, especially one longer than 12 hours.

Hardening The process of disabling unnecessary services, installing all the latest patches, installing security software (*e.g.*, anti-virus software), tuning the operating system, and documenting the system.

Hash Mathematical formula that generates code from a message.

Header Portion of a packet (refer to packet definition), which contains the source and destination addresses, error checking information, message originator, date and time, and subject lines.

High-Level Format The process of formatting using the FORMAT command in Windows or DOS performs a high-level format. This does not destroy the data on the disk. This process simply resets the index in the file allocation table so that the operating system sees the disk as empty.

Hoax E-mail messages that are usually untrue and flood the Internet. Instead of spreading from one computer to another by itself, hoaxes rely on people to pass them along.

Host A single computer or workstation, may be connected to a network.

Identification The process of determining who a user claims to be; usually performed by presenting a user ID (*i.e.*, “jsmith”).

Impersonation Pretending to be authorized to enter a secure location.

Industrial Espionage The act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies).

Information Assurance Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Custodians Individuals (*e.g.*, IT staff) who maintain or administer information resources on behalf of Information Owners. They are guardians or caretakers who are charged with the resource owner’s requirements for processing, telecommunications, protection controls, and output distribution for the resource.

Information Owners 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.

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

Information Security (InfoSec) Those measures, procedures, and controls which provide an acceptable degree of safety of information resources from accidental or intentional disclosure, modification, or denial of service, whether in storage, processing, or transit.

Information Technology Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement control, display, switching, interchange, transmission, or reception of data or information.

Integrity Assuring information will not be accidentally or maliciously altered or destroyed. Information has integrity when it is timely, accurate, complete, and consistent.

Interface A program or device which connects programs and/or devices.

Intruder An unauthorized user or unauthorized program, generally considered to have malicious intent, on a computer or computer network.

Intrusion Any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource through unauthorized access or penetration of an information resource.

Intrusion Detection System A system that analyzes network traffic to detect anomalies and provide alerts regarding possible intrusions.

IP address A 32-bit binary address used to identify a host's network ID.

IP Spoofing An attack whereby a system attempts to illicitly impersonate another system by using IP network address.

Iris Recognition Eye biometric that focuses on the unique characteristics found in the iris.

ISDN A type of communication line which can carry voice, digital network services and video.

Isolated computer A computer which is not connected to a network or any other computer; a stand-alone personal computer is an example.

Key A symbol or sequence of symbols (or electrical or mechanical correlates of symbols) applied to text in order to encrypt or decrypt.

Key Escrow The system of giving a piece of a key to each of a certain number of trustees such that the key can be recovered with the collaboration of all the trustees.

Keyboard Attack Extracting information from data storage media by executing software utilities, keystrokes, or other system resource executed from a keyboard. For example, disk and file recovery utilities and memory scavenging procedures can be used to carry out keyboard attacks.

Keystroke Monitoring A specialized form of audit trail software, or a specially designed device, that records every key struck by a user and every character of the response that the AIS returns to the user.

Lab Network Any network used for the purposes of testing, demonstrations, training, etc. Any network that is stand-alone or firewalled off from the production network(s) and whose impairment will not cause direct loss to OPIC nor affect the production network.

Lawful Permanent Resident. Any individual who is not a citizen or national of the United States who has been lawfully admitted into the United States and accorded the privilege of residing permanently in the U.S. as an immigrant in accordance with the immigration laws, such status not having changed.

LDAP (Lightweight Directory Access Protocol) A standardized way to connect with a directory which might hold passwords, addresses, public encryption keys, and other exchange-facilitating data.

Legacy System Older software and hardware systems still in use and generally proprietary.

LISTSERV Commercial mailing list. Although LISTSERV refers to a specific mailing list server, the term is sometimes used incorrectly to refer to any mailing list server.

Local Area Network (LAN) A local computer communications system that connects information resources within a building or group of buildings within a few square kilometers, including workstations, front-end processors, controllers, switches, and gateways.

Log files Files that show the status of the system and are accessed via Event Viewer, which lists the severity and a brief description of the logged event.

Login script A set of stored commands that can log a user into a computer automatically.

Logon ID A character string that uniquely identifies a user on a computer system.

Low-Level Format This process will destroy all data on the disk. The FORMAT command in DOS or Windows does not perform a low-level format.

Macro A computer program containing a set of procedural commands to achieve a certain result.

Major Information System An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Malicious Code Any software or firmware that is intentionally included in a system for an unauthorized purpose. Examples include viruses like Trojan horses, worms, and scripts used by crackers/hackers to gain privileges, capture passwords, and to modify audit logs to hide unauthorized activity Information given to you when you log into or otherwise access a system.

Malicious Hackers People who break into computers without authorization, and may be either outsiders or personnel internal to OPIC.

Management Controls Security techniques and concerns that normally focus on the management of the computer security program and the management of risk within the organization.

Media Physical objects on which data can be stored, such as hard drives, zip drives, floppy disks, compact disks, CD-ROMs, DVDs, flash drives, and tapes.

Memory Cards Removable electronic storage devices, which do not lose the information when power is removed from the card.

Memory Scavenging Searching through data storage to collect residue thereby acquiring data. Data may be stored on records, blocks, pages, segments, files, directories, words, bytes, fields, or peripheral devices, such as printers or video displays.

Metadata Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted. There are at least three types of metadata: semantic data, which gives the meaning of the "raw" data; formatting data which describes the appearance of the data on-screen or on-page; and intellectual property data which describes data ownership conditions.

Minimal Additional Expense Employee's personal use of Government office equipment is limited to those situations where the Government is already providing equipment or services and the employee's use of such equipment or services will not result in any additional expense to the Government or the use will result in only normal wear and tear or the use of small amounts of electricity, ink, toner or paper. Examples of minimal additional expenses include, making a few photocopies, using a computer printer to print a few pages of material, infrequently sending personal E-mail messages, or limited use of the Internet for personal reasons.

Mobile Computing Device A laptop, PDA, or other *portable* device that can store or process data.

Modem A device that enables a computer to transmit data over telephone lines by converting data between the computer's digital format and the phone line's analog format.

Network Two or more machines interconnected for communications.

Network Device Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

Network Mapping A probe that uses SNMP or broadcast ICMP "ping" packets to determine the architecture of your network.

Network Security Protection of networks and their services from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side-effects.

Network Sniffer (or Packet Sniffer), Network-monitoring program used to capture information transferred across a network.

Node In a network, a node can be a computer or some other device such as a printer. Every node has a unique network address.

Noise Any unwanted electrical signal.

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.

Operational Controls Security measures that are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems), are generally procedural in nature.

Operational Data Security The protection of data from either accidental or unauthorized, intentional modification, destruction, or disclosure during input, processing, or output operations.

Overwriting Process of writing patterns of data on top of the data stored on a magnetic medium.

Packet Limited-length unit of data formed by the network, transport, presentation, or application layer (layers 3-7 of the OSI Model) in a networked computer system. Data is transported over the network, and larger amounts of data are broken into shorter units and placed into packets.

Packet Filtering A feature incorporated into routers and firewalls to limit the flow of information based on pre-determined communications such as source, destination, or type of service being provided by the network. Packet filters let the administrator limit protocol specific traffic to one network segment, isolate email domains, and perform many other traffic control functions.

Packet Filtering Firewalls Firewalls which use rules based on a packets source, destination, port or other basic information to determine whether or not to allow it into the network.

Packet Sniffer A device or program that monitors the data traveling between computers on a network.

Passive Attack Attack which does not result in an unauthorized state change, such as an attack that only monitors and/or records data.

Passive Threat The threat of unauthorized disclosure of information without changing the state of the system. A type of threat that involves the interception, not the alteration, of information.

Password Any secret string of characters which serves as authentication of a person’s identity, and which may be used to grant or deny access.

Password Guessing Attack A computerized or manual process whereby various possible passwords are provided to a computer in an effort to gain unauthorized access.

Password-based Access Control Software that relies on passwords as the primary mechanism to control system privileges and logging activities.

Patch A patch is a 'fix' to a known problem with a piece of software. Instead of redistributing the entire new version of a program a patch, which is much smaller, can be applied to the old version.

Penetration 1.The successful unauthorized access to an information resource; 2. The act of bypassing the security mechanisms of a network or system.

Penetration Testing The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators work under the same constraints applied to ordinary users.

Perimeter Based Security The technique of securing a network by controlling access to all entry and exit points of the network. Usually associated with firewalls and intrusion detection systems.

Personal Firewall Software installed on a computer or device which helps protect that system against unauthorized access.

Personal use Activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

Personnel Security The procedures established to ensure that all personnel who have access to any classified information have the required authorizations as well as the appropriate clearances.

Physical Security The measures used to provide physical protection of resources against deliberate and accidental threats.

Piggybacking 1. Unauthorized access to information by using a terminal that is already logged on with an authorized ID; 2. Entering secure premises by following an authorized person through the security perimeter.

Plaintext Unencrypted data.

Platform Underlying hardware or software for a system.

Portal A gateway or single point of entry through which the user can access related information from a variety of sources.

Private Branch Exchange (PBX) A private telephone switchboard that provides on-premises dial service and may provide connections to public communications networks.

Private Key Cryptography An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret.

Privilege An authorized ability to perform a certain action on a computer, such as read a specific computer file.

Privileged user-ID A userid that has been granted the ability to perform special activities, such as shut down an application or system.

Production Application A tested, documented, and periodically-executed computer program which performs one or more regular business activities related to OPIC's mission

Production Network The "production network" is the network used in the daily business of OPIC. Any network connected to the corporate backbone, either directly or indirectly. Any network whose impairment would result in direct loss of functionality to OPIC's employees or impact their ability to do work

Protocol Agreed-upon methods of communications used by computers. A specification that describes the rules and procedures that products should follow to perform activities on a network, such as transmitting data.

Proxy A software agent that acts on behalf of a user, typical proxies accept a connection from a user, make a decision as to whether or not the user or client IP address is permitted to use the proxy, perhaps does additional authentication, and then completes a connection on behalf of the user to a remote destination.

Public Key Infrastructure (PKI) A system for securely exchanging information within a company, group or worldwide 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. A coding system in which encryption and decryption are done with public and private keys, allowing users who don't know each other to send secure or verifiable messages. This method, also known as dual-key cryptography, contrasts with Private Key Cryptography or symmetric cryptography, in which the sender and recipient must agree on and use the same private key for encryption and decryption.

Record A complete set of information (fields) for a particular item in a database.

Recovery The phase in Incident Handling that returns the system to a fully operational status.

Remanence Residual information remaining on data storage media after clearing.

Remote Access Any access to OPIC's corporate network through a network, device, or medium that is not controlled by OPIC (such as the Internet, public phone line, wireless carrier, or other connectivity).

Residual Data Information that appears to be gone, but is still recoverable from the computer system and includes "deleted" files still extant on a disk surface and data existing in other system hardware such as buffer memories of printers and fax machines.

Retention schedule A management-approved listing of the types of information that must be retained for archival purposes and the time frames that these types of information must be kept.

Risk The possibility of something adversely affecting the confidentiality, availability and integrity of OPIC’s information resources.

Risk analysis
An evaluation of system assets and their vulnerabilities to threats. Risk analysis estimates potential losses that may result from threats.

Risk Assessment
1. The process of analyzing and interpreting risk. Risk assessment is used to identify security risks, examine threats to and vulnerabilities of systems, determine the magnitude of risks, identify areas needing safeguarding, and determine the acceptability of risk; 2. A study of vulnerabilities, threats, likelihood, loss or impact, and theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Risk Management
1. The process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. The risk management process allows OPIC to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support the agency’s mission. 2. The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk management program is to reduce risk and obtain and maintain DAA (Designated Approving Authority) approval. 3. Decisions to accept exposure or to reduce vulnerabilities by either mitigating the risks or applying cost effective controls.

Root
The root directory of a computer system or a device is the directory that directly or indirectly contains all the other directories in the computer system or on the device.

Router
A device that interconnects networks; used in some instances to provide access control and message routing services.

Sanitize
To expunge data from storage media (e.g., diskettes, CD-ROMs, and tapes) so that data recovery is impossible. Sanitizing includes overwriting, degaussing and destruction.

Scalable
Describes how well a system can be adapted and expanded to meet increased demands.

Secure Sockets Layer (SSL)
A session layer protocol that provides authentication and confidentiality to applications.

Security
A condition that results from the establishment and maintenance of protective measures that ensure a state of inviolability from hostile acts or influences.

Security administrator
The person charged with monitoring and implementing security controls and procedures for a system.

Security Architecture
A detailed description of all aspects of the system that relate to security, along with a set of principles to guide the design. A security architecture describes how the system is put together to satisfy the security requirements.

Security Controls
Hardware, programs, procedures, policies, and physical safeguards, which are put in place to safeguard information and the means of processing it.

Security Countermeasures
Protections that are aimed at specific threats and vulnerabilities or involve more active techniques.

Security Features
The security-relevant functions, mechanisms, and characteristics of an information resource

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.

Security Policies The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements Types and levels of protection necessary for equipment, data, information, applications, and facilities.

Security Violation An instance in which a user or other person circumvents or defeats the controls of a system to obtain unauthorized access to information contained therein or to system resources.

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

Sensitive Information 1. Any information, the disclosure of which could damage OPIC, business partners, customers, or other third parties; 2. Any information the loss, misuse, or unauthorized access to, or modification of, could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under The Privacy Act, but which has not been specifically authorized under criteria established by Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

Separation Of Duties Concept which provides the necessary checks and balances to mitigate against fraud, errors, and omissions by ensuring that no individual or function has control of the entire process

Server Computer that provides a service or application that users access through a network connection.

Smart Card A device that is similar in size to a credit card but that has the capability to store data and perform processing of information.

Sniffer A device/program used to capture data passing through a network.

Spam Unauthorized and unsolicited electronic mass mailings.

Split Tunneling Simultaneous direct access to a non-OPIC network (such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into OPIC's corporate network via a VPN tunnel.

Spoofing The creation of IP packets with counterfeit IP source addresses.

Standard A procedure or control mechanism that is required to be used in specific situations.

Steganography The art and science of communicating in a way that hides the existence of the communication. It is used to hide a file inside another. For example, an image can be hidden inside another graphic image file, audio file, or other file format.

Strong Authentication An authentication process using techniques which would require a high level of effort to compromise and are not subject to compromise by eavesdropping. Strong authentication processes may use challenge/response password devices, SmartCards, or one-time passwords.

Switch A physical component that connects multiple computers and devices to a network

System Administrator A designated individual who has special privileges to maintain the operation of a computer application or system.

System control data Data files such as programs, password files, security tables, authorization tables, etc., which if not adequately protected, could permit unauthorized access to information resources

System integrity The requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system."[2]

TCP/IP Transmission Control Protocol/Internetwork Protocol. The suite of protocols the Internet is based on.

Technical Controls Security measures that are executed by the computer system. These controls are dependent upon the proper functioning of the system for their effectiveness.

Telephony The technology associated with the electronic transmission of voice, fax, or other information between distant parties using systems historically associated with the telephone.

Telnet Protocol that allows you to connect across the Internet and to log onto another computer as if you were connected directly.

Threat A circumstance, event, or person with the potential to cause harm to a system in the form of destruction, disclosure, data modification, and/or Denial of Service (DoS).

Threat Assessment Process of formally evaluating the degree of threat to an information system and describing the nature of the threat.

Timestamp The date and time signature of when that specific file was saved to the computer's memory.

Topology The map or plan of the network. The physical topology describes how the wires or cables are laid out, and the logical or electrical topology describes how the information flows.

Trace Packet In a packet-switching network, a unique packet that causes a report of each stage of its progress to be sent to the network control center from each visited system element.

Trapdoor Hidden flaw in a system mechanism that can be triggered to circumvent the system's security.

Trojan Horse A malicious program that disguises itself as a beneficial or entertaining program but that actually damages a computer or installs code that can counteract security measures (perhaps by collecting passwords) or perform other tasks (such as launching a distributed denial of service attack). Unlike a computer virus, a Trojan horse does not replicate itself. Intruders use Trojan horse programs to hide their activity, capture username and password data, and create backdoors for future access to a compromised system. A "Time Bomb" is a Trojan horse set to trigger at a particular time.

Trusted Computing Base The totality of protection mechanisms within a computer system including hardware, firmware, and software - the combination of which are responsible for enforcing a security policy. A TCB consists of one or more components that together enforce a unified security policy over a product or system.

Unauthorized Access The use of an information resource without permission

Un-Trusted Network Any network firewalled off from the corporate network to avoid impairment of production resources from irregular network traffic (lab networks), unauthorized access (partner networks, the Internet etc.), or anything else identified as a potential threat to those

[2] National Computer Security Center, Pub. NCSC-TG-004-88.

resources.

User A person that uses Information Technology resources

UserID Character string that uniquely identifies a computer user or computer process.

Users Individuals who use or have access to information resources, including employees, vendors, and visitors.

Validation 1. Tests to determine whether an implemented system fulfills its requirements. 2. The checking of data for correctness or for compliance with applicable standards, rules, and conventions. 3. The process of applying specialized security test and evaluation procedures, tools, and equipment needed to establish acceptance for usage of an information system.

Verification The process of ensuring that information has not been changed in transit or in storage, either intentionally or accidentally.

Virtual Private Network (VPN) A method for establishing a secure virtual channel ("tunnel") through an unsecured network (such as the Internet) through the use of encryption.

Virus A malicious program which, when executed, copies itself onto other media or files available to the computer executing it and may cause damage to a computer system by attacking or attaching itself to boot information, email, data file, or another program.

Vulnerability Any characteristic of a computer system that renders it susceptible to destruction or incapacitation. A design, administrative, or implementation weakness or flaw in hardware, firmware, or software that, if exploited (either intentionally or accidentally), could lead to an unacceptable impact in the form of unauthorized access to information or disruption of critical processing.

Vulnerability Assessment Systematic examination of a network or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Web Site Defacement The malicious modification of a Web site.

Wide Area Network (WAN) A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks

Wipe Slang term for deliberately overwriting a piece of media and removing any trace of files or file fragments.

Worm Independent program that replicates from machine to machine across network connections often clogging networks and information systems as it spreads, perhaps causing denial of service.