Overseas Private Investment Corporation

Information Resources Management

INFORMATION SYSTEMS SECURITY

PROGRAM PLAN

Draft Version 3

January 14, 2003

TABLE OF CONTENTS

1 INTRODUCTION

The Overseas Private Investment Corporation (OPIC) was established as an agency of the US government in 1971. OPIC helps US businesses invest overseas, fosters economic development in new and emerging markets, complements the private sector in managing risks associated with foreign direct investment, and supports US foreign policy. Because OPIC charges market-based fees for its products, it operates on a self-sustaining basis at no net cost to taxpayers. The OPIC staff consists of approximately 220 employees, all based at 1100 New York Avenue, N.W. in Washington, DC.

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

As a federal entity, 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 1 illustrates some of the threats that exist to federal 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.

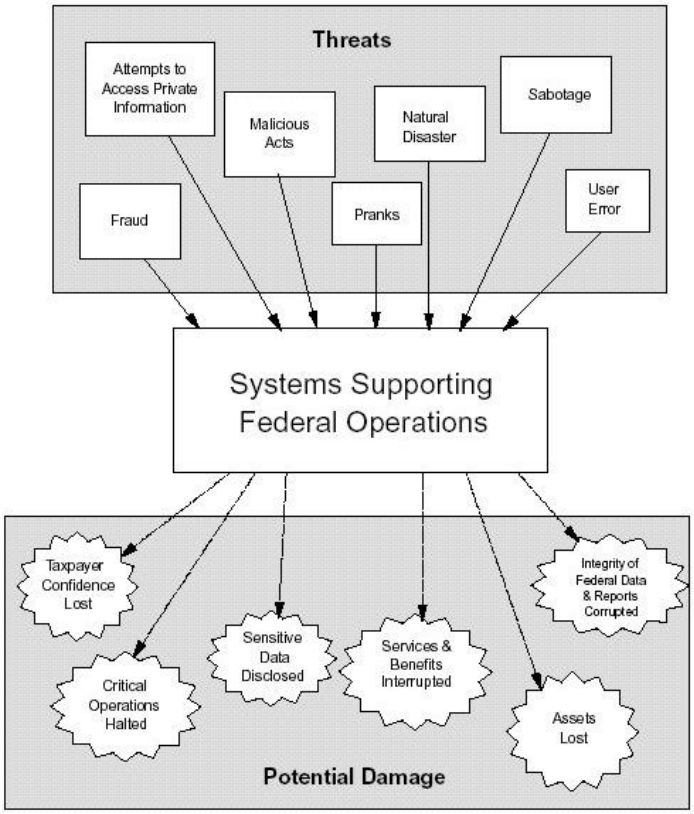


Figure 1: Threats to Federal Systems[1]

The primary goal of the OPIC Information Systems Security Program (ISSP) is to mitigate these threats and vulnerabilities by preventing them or minimizing 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 be at risk of liability for not preventing exposure of the resources with which it has been entrusted.

Effective information assurance is not the ISSP's only goal, however. As a federal agency, OPIC is required to conform to federal standards, regulations, and directives that govern information security. OPIC's information security program is subject to audits and reviews by a variety of organizations, including the General Accounting Office (GAO), the Office of Management and Budget (OMB), and other entities. Under the Federal Information System Management Act (FISMA), OPIC must provide periodic reporting to OMB regarding audit findings, and deliver a schedule of remediation in the form of a Plan of Action and Milestones (POA&M). Other federal regulations dictate additional safeguards, management practices, and reporting requirements with which OPIC must comply. The agency must also follow federal standards, such as the National Institute of Standards and Technology (NIST) 800 series, and participate in federal information security cooperative initiates, such as sharing information with FedCIRC.

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

OPIC is committed to developing an effective ISSP that is fully compliant with FISMA and other federal regulations and standards, adheres to industry best practices, and is tailored to OPIC business needs. This document outlines the plan for implementing the ISSP, which includes the following key initiatives:

- Develop Information Security policies
- Create a Security Training and Awareness Program
- Setup an Incident Management capability
- Implement Risk Management practices, including:
    - Classification Framework
    - Risk Assessments
    - Certification and Accreditation program
    - Periodic vulnerability testing
    - Integration of security into IT Decision Making and the Systems Development Lifecycle
- Develop a System Security Plan for OPICNET
- Perform Continuity of Operations Planning
- Institutionalize OPIC Information Security roles and responsibilities
- Address existing known vulnerabilities

2 OBJECTIVES

The purpose of this document is to provide a plan for implementing an ISSP that provides protection for OPIC information resources and also conforms to federal requirements and guidelines. This plan utilizes existing federal methodologies and frameworks (where available) and industry best practices to create a security program customized to the OPIC business environment.

In particular, this document will:

- Describe the major components that will comprise the OPIC ISSP;
- Outline the tasks that need to be performed to develop and implement the program;
- Provide a schedule for performing these tasks;
- Specify roles and responsibilities; and
- Discuss the security program management approach.

3 CRITICAL SUCCESS FACTORS

The following factors are critical to the success of this plan:

- OPIC executives will provide support and endorsement for information security and the initiatives described in this plan.
- The ISSO will have timely access to OPIC departmental representatives to discuss the departments' information resource usage and security needs.
- OPIC management and Human Resources personnel will provide assistance with enforcement of information security policies.
- Human Resources personnel will assist with implementation of the information security training program (including its incorporation into the employee orientation process).
- Documents will be reviewed, and feedback provided to the ISSO, in a timely fashion.

4 METHODOLOGY

An effective information assurance program is composed of many elements. These include a variety of policies, processes, and technical components that must be integrated in a coordinated fashion. While methodologies and guidelines exist for many of the security program elements, they must be tailored and applied to OPIC's specific environment and business needs. The following sections describe the primary elements that will comprise the OPIC ISSP and the steps that will be taken to implement them.

4.A Security Policies

Security policies form the foundation of good security practice. Policies provide the basic rules for an organization to operate securely. Because the primary purpose of a security program is to protect the agency and its clients, security policies must be aligned with Corporate goals. For example, policies tell employees how they may use the organization's IT resources and what resources the organization considers critical to protect. It is also important that these rules are clearly defined and documented, and that everyone within OPIC understands them. Additionally, someone must have the authority and responsibility to enforce the policies.

Policy statements themselves are generally fairly broad and generic in order to provide flexibility and long-term applicability. For example, an OPIC information security policy might state that users must be authenticated to systems in order to use them, without stating the specific method of authentication that must be used. Standards, Guidelines, and Procedures are then used to provide details regarding how the policies should be implemented and used. Standards specify use of particular technologies in a particular way (such as standard operating procedures) and are usually compulsory. Guidelines are general recommendations for applying security practices. Procedures provide step-by-step instructions for adhering to standards and policies. An example of a procedure would be OPIC's process for removing system accounts when an employee leaves the organization.

The first step in developing the OPIC ISSP will be to develop a comprehensive set of information security policies, along with appropriate standards, guidelines, and procedures for their usage. The OPIC security policies will be derived from federal guidelines and best practices, and tailored in accordance with OPIC-specific business need.

Specific steps that will be completed to develop the OPIC Information Security policies include:

- Create security policy framework and templates;
- Analyze federal guidelines and best practices, along with OPIC business needs, to determine appropriate policies for OPIC IT environment;
- Compose formal policies, standards and guidelines;
- Develop procedures for periodic review and update of policies, standards and guidelines;
- Update OPIC Information Systems Security Handbook to reflect the new policies, standards, and guidelines;
- Communicate policies to OPIC personnel and contractors.

4.B Security Training and Awareness

An important aspect of information security is ensuring that everyone at OPIC understands not only the security policies that apply to them, but also their own role in maintaining information security, and the consequences of non-compliance. They must also understand why security should be important to both OPIC and themselves. OPIC personnel and contractors must have a basic understanding of the security risks in their IT environment and what they can, and are expected, to do to help protect the OPIC's resources.

OPIC will develop a Security Training and Awareness program to educate personnel about information security and the policies and procedures with which they must comply. This will include both periodic training classes and an ongoing security awareness campaign designed to ensure that employees maintain vigilance. Similar to the OPIC Ethics program, Security training should become part of the orientation program for new personnel and provide mandatory periodic refresher training. This program will be based on the NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" guidelines and industry best practices, and will incorporate OPIC-specific information security policies and practices.

The steps for building OPIC's Information Security Training and Awareness program will include the following:

- Develop training program:
  - Determine curriculum;
  - Develop training materials and delivery mechanism;
  - Perform training for current personnel;
  - Perform additional security training for information custodians (i.e. enhanced security training for system administrators)
  - Incorporate security awareness training into new employee (and contractor) orientation program; and
  - Institute process for periodically updating training materials and providing refresher training to users.
- Create IT Security awareness campaign:
  - Determine security messages and identify delivery mechanisms;
  - Create materials;
  - Implement/distribute awareness materials; and
  - Provide for periodic update and redistribution of security awareness materials.

4.C Incident Management

Incident Management is the process of handling security incidents that occur. A security incident is any activity that occurs that is a threat to the security of information resources. These can be either intentional or accidental events that jeopardize the availability, integrity or confidentiality of the organization's information and systems. Examples include computer virus attacks, loss of power to the computer center, unauthorized access to resources, and accidental exposure of sensitive information, all of which have recently occurred in the OPIC environment.

Incident Management is composed of several functions:

- *Detection* – Determining through automated alerts, personnel experience, or other monitoring that an incident has occurred. For example, this could be a user noticing they cannot access a system, or a monitoring system noticing a fault.

- *Internal Reporting* – Communicating the incident situation to appropriate incident handling contacts. For example, this could be a user calling the Help Desk or a monitoring system sending an alert to someone's pager.

- *Response* – Handling the incident to minimize impact. For example, this could be stopping an intruder, restoring access to a resource, and/or investigating a system anomaly.

- *Documentation* – Tracking what happened, how it was handled, and any future actions that should occur.

- *External Reporting* – Informing law enforcement, FedCIRC, and/or other applicable outside entities as needed.

OPIC has developed a procedural format for reporting and tracking incidents. Further refinement of these procedures, including detailed instructions for users and IT personnel, will be performed. Additional procedures for responding to and externally reporting incidents will also be developed.

Specifically, development of the Incident Management program will include:

- Develop guidelines regarding what constitutes an incident;

- Specify roles and responsibilities for incident reporting and response;

- Create instructions and mechanisms for reporting incidents to the appropriate internal authorities;

- Develop and implement procedures for processing incident reports that have been received internally. This includes investigating, correcting, and fully documenting the incident; and

- Develop and implement procedures for reporting incidents to FedCIRC and other appropriate contacts (such as law enforcement).

4.C.I Coordination with FedCIRC

Informal procedures have already been implemented for reporting incidents to FedCIRC and law enforcement. OPIC is currently working to develop a signed agreement and more formal procedures for cooperation with FedCIRC. Specifically, OPIC plans to:

- Finalize and sign a cooperative agreement with FedCIRC;
- Implement more formal procedures for providing information to FedCIRC; and
- Develop and implement procedures for handling information provided by FedCIRC and for obtaining assistance from FedCIRC when needed.

4.D System Security Plan

A System Security Plan (SSP) is a document that provides an overview of the security requirements applicable to the system and specifies the protection mechanisms implemented to meet those requirements and safeguard the system. The SSP also specifies roles and responsibilities regarding secure usage of the system. Each major system in an organization should have an SSP.

As a small agency, OPIC has a single major IT system, "OPICNET," which contains all of the agency's critical infrastructure components. A security plan will be developed for OPICNET in accordance with NIST Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," and other best practice guidance.

The OPICNET Security Plan will include:

- An inventory of the hardware and software components that compose OPICNET;
- Specification of interfaces and connections with other systems;
- Assessment of the risks associated with OPICNET;
- Analysis of security requirements that apply to OPICNET;
- Description of security controls (current and planned) to manage the identified risks and fulfill the security requirements; and
- Delineation of roles and responsibilities for usage of the system.

4.E Risk Management

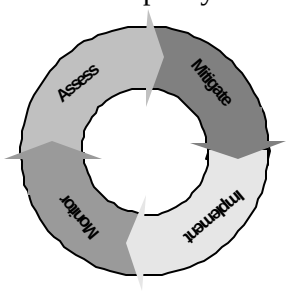
In determining a security strategy for a system or the organization, OPIC must determine the correct balance between mitigating risks and expending resources. Appropriate controls must be implemented to protect against the occurrence of serious threats to the business while addressing financial and operational concerns. Risk Management is the process of assessing each risk, determining the appropriate mitigation strategy, and ensuring that the mitigation strategy is implemented effectively.

Each risk must be assessed based on the likelihood of the risk occurring, the potential impact that the risk would have if it were to occur, and the cost to OPIC to mitigate the risk. Based on this analysis for each risk, OPIC may decide to:

- Mitigate the risk, using technology, policy, and/or management/procedural controls;
- Accept the risk, if the impact is minor compared to the cost of mitigation; or
- Transfer the risk to another party, such as through use of an insurance policy.

Risk management is a multiphase process:

1. Identify and assess potential risks
2. Determine mitigation strategies for the risks
3. Implement the mitigation strategies
4. Monitor for effectiveness of mitigation controls



This process is also a cyclical one. Risk management is an ongoing process that must be continuously readdressed to provide maximum effectiveness.

OPIC's Risk Management program will be composed of several key components, which are described below:

- Classification framework
- Risk Assessment process
- Periodic vulnerability testing
- Certification and Accreditation program
- Integration of risk management into the systems development lifecycle
- Risk-based decision making

OPIC has completed a self-assessment and had an independent vulnerability assessment performed by NetSec. A POA&M has been developed to address vulnerabilities and weaknesses discovered by these assessments.

The NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems", framework will serve as the guiding methodology for developing the OPIC Risk Management program.

4.E.I Classification Framework

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.

OPIC's classification framework will be based on the FIPS Publication 199, "Standards for Security Categorization of Federal Information and Information Systems"[2], standard and will be used to classify existing and future OPIC information resources.

[2] National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) #199, Draft 9/18/2003

4.E.II Risk Assessment

Risk Assessment is the process of analyzing the risks to information resources. This analysis includes determining what risks exist, the likelihood of those risks occurring, and the impact on the organization if those risks were to occur. This information can then be used to make intelligent decisions regarding the levels of protection needed.

OPIC's Risk Assessment process will be based on the NIST Special Publication 800-30, "Risk Management Guide for Information Technology Systems", methodology.

The tasks for developing a Risk Assessment framework at OPIC include:

- Develop strategy, guidelines, and templates for assessing risks to IT systems;
- Implement tools as necessary;
- Document policies and procedures to periodically assess risks of OPIC's IT systems; and
- Periodic review of security controls:
    - Adequacy/Relevance
    - Functioning as Designed.

4.E.III Vulnerability Testing

Vulnerability testing is the process of scanning systems to look for weaknesses that could result in security shortfalls. The purpose is to identify areas of risk so that they may be appropriately analyzed and mitigated.

To implement vulnerability testing, OPIC will call upon NIST Special Publication 800-42, "Guideline on Network Security Testing" and other standard procedures and tools. The following steps will be performed to provide periodic vulnerability testing of OPIC information resources.

- Determine scope of testing;
- Plan strategy and process for testing;
- Select and acquire tools;
- Create detailed procedures;
- Perform initial testing;
- Optimize testing procedures process;
- Implement periodic testing; and
- Create plan for periodic update of testing process.

4.E.IV Integrating Risk Management into the Systems Development Lifecycle

To maximize effectiveness and minimize cost, Security should be integrated throughout the system development lifecycle. This includes the incorporation of security into all stages, such as requirements, design, testing, operation, change, and

removal of the system. The implementation of the AIM system would be a good opportunity to start incorporating these principles into the OPIC environment.

Following the NIST Special Publication 800-64 methodology, "Security Considerations in the Information System Development Life Cycle", OPIC will implement policies and procedures for incorporating risk management into each phase of the system lifecycle. This will include performing the following tasks:

- Determine and implement plan for incorporating security into the OPIC systems development lifecycle;
- Develop OPIC-specific procedures related to new systems and system changes; and
- Create a process for authorization, testing, and approval of system software and hardware;

4.E.V Risk-Based Decision Making

Risk-Based Decision Making (RBDM) is a process by which management makes informed decisions based on risk analysis. In terms of information security, this means that decisions regarding the selection, implementation, and usage of information resources are made based on the degree and acceptability of their associated risk. Essentially, RDBM incorporates Risk Management into the IT decision process. Therefore implementing RDBM at OPIC involves first implementing an Information Risk Management process (as described above) and then incorporating the usage of this process into management decision-making regarding the acquisition and usage of information resources.

4.E.VI Certification and Accreditation

The purpose of Certification and Accreditation (C&A) is to ensure that 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 determine whether the system's security needs are being met. Specifically, Certification is an assessment of the security controls of the system, and Accreditation is a risk-based decision made based on the certification. Security Testing & Evaluation (ST&E) is the process of testing security measures during the Certification process.

OPIC will develop a C&A process based on the NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems", methodology. Once implemented, this process will be utilized to certify and accredit the OPICNET system.

Tasks that will be performed to implement C&A at OPIC include:

- Develop processes and templates;
- Define and assign responsibilities;
- Create procedures for documenting and evaluating system security;
- Develop procedures for ST&E; and
- Perform C&A of OPICNET.

4.F Continuity of Operations Planning

OPIC's IT resources are vulnerable to a variety of disruptions, ranging from temporary power outages to facility disasters. While the risks of these events occurring can be reduced through security controls, they cannot be completely eliminated. Thus, it is essential to have a plan for providing access to critical information resources in the event of such a disruption. Additionally, it is imperative to keep this plan updated so that it does not become obsolete or ineffective. It is also vital to test the plan periodically, to ensure that the procedures are accurate and sufficient and also to provide practice in its implementation as preparation for an emergency situation.

OPIC currently has a Continuity Of Operations Plan (COOP) but it has not been implemented. OPIC will review, update and test this plan to ensure that essential information resources will be available in the event of an emergency. Additionally, processes will be implemented to periodically review, update, and test the plan.

Specific tasks that will be performed include:

- Identify mission-critical information resources;
- Review existing COOP plan;
- Develop IT Disaster Recovery Plan and Continuity of Support Plan;
- Perform testing of the plans;
- Update the plans and testing procedures based on results of the testing; and
- Create procedures for periodic update and testing of the plans.

The NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems", will provide the framework for developing these plans.

5 ROLES AND RESPONSIBILITIES

Everyone at OPIC shares in the responsibility of protecting the organization's critical information resources and adhering to the agency's policies on their usage. However, the Information Resources Management (IRM) division within the Office of the Chief Financial Officer (OCFO) bears the primary responsibility for developing, implementing, and operating the OPIC ISSP.

IRM is charged with the mission "to bring business agility to the corporation through the delivery of superior IT business solutions and services." The Group is responsible for 1) developing, maintaining and facilitating the implementation of a sound and integrated information architecture for OPIC and 2) promoting the effective and efficient design and operation of all information resource management processes, including work process improvements, and managing contractor provided Customer support. This includes development and operation of an ISSP.

Within IRM, the following positions hold specific responsibilities regarding the safeguarding of OPIC information resources.

5.A Chief Information Officer (CIO)

The Chief Information Officer (CIO) oversees the programs of Information Resources Management in order to design, develop and implement comprehensive corporate information systems. The CIO plans the nature and extent of IT operations and activities for OPIC, and ensures that IT management directly supports OPIC's strategic mission. The CIO promotes a coordinated, interoperable, secure and shared corporate IT infrastructure. The CIO also monitors and evaluates the performance of information systems on the basis of applicable performance measures and customer service, develops and implements plans for improving overall program activities, develops OPIC IT directives to implement congressional and executive policy actions, and participates in the investment review process for information systems. Additionally, the CIO serves as a corporate-wide resource for major policy, program, or operational initiatives, and provides advice on technical information technology issues that may impact the creation and maintenance of cooperative agreements with customers and stakeholders.

Per the Federal Information Security Management Act (FISMA) and OMB implementing directives, the CIO monitors, evaluates and reports the status of information security within the Agency to the President and Chief Executive Officer of OPIC. The CIO also assigns information ownership responsibility and acts as the Designated Approving Authority (DAA) for OPIC information systems.

5.B Director of Technical Services (DTS)

The Director of Technical Services (DTS) provides management and leadership for planning, delivery, and maintenance of OPIC corporate infrastructure services and is responsible for the day-to-day operations of the Service Delivery team, including coordination of an integrated suite of network, end-user access, wireless, and information services. The DTS provides guidance and direction to a number of functional teams and team leaders in delivering core business functions such as: customer service, systems engineering and implementation, operations and maintenance. Additionally, the incumbent works collaboratively with other department managers and corporate management to ensure efficient and cost-effective infrastructure solutions and services in support of corporate and departmental needs.

As part of his duties, the DTS oversees the development and operation of the ISSP, and ensures integration of the program with other IT initiatives, procedures, and strategic plans. The DTS also acts as liaison with OPIC upper management regarding approval and status of OPIC information security policies and practices.

5.C Information Systems Security Officer (ISSO)

The ISSO is assigned to the Information Resources Management (IRM) group and reports to the Director of Technical Services. The primary responsibilities of the ISSO are to develop, implement and maintain an ISSP within OPIC, and to ensure the confidentiality, integrity and availability of information and information systems through formal policies, awareness training, monitoring compliance and access controls. The ISSO identifies and assesses risk, explores controls and countermeasures, provides recommendations to senior management, develops and obtains senior management approval of policies and procedures, and implements approved policies and procedures. This person acts to a) protect the privacy and confidentiality of data; b) help ensure reliable service to those dependent on OPIC information resources; and c) prevent waste and abuse of Government resources. To this end the ISSO advises the CIO and other senior management on these issues.

6 PROGRAM MANAGEMENT & REPORTING

Progress against this plan will be closely tracked and reported on a regular basis. This will be facilitated by the following activities:

- The program work breakdown, shown in Section 7, will be updated on a regular basis to track progress against the plan.
- Monthly briefings will be provided to OPIC executives regarding the status of implementing the ISSP as well as the operational status of OPIC information security. This will include a report of
    - Progress against program milestones;
    - Significant accomplishments and activities;
    - Issues and risks; and
    - Operational statistics (such as number of security incidents).
- OPIC IRM management will play an integral role in reviewing and approving all policies, plans, procedures and technical measures implemented as part of the ISSP.
- Peer reviews will also be performed as part of the development of each program element in order to provide Quality Assurance.
- All security incidents will be tracked and reported as they occur. Critical incidents will be immediately brought to the attention of OPIC management. Additionally, these reports will be provided to FedCIRC and other appropriate parties.
- OPIC will provide regular reports to OMB regarding the organization's progress against the tasks outlined in the POA&B, as required by FISMA.
- An annual independent evaluation of the OPIC ISSP will be performed as required by FISMA.

7 SCHEDULE

Based on this plan, OPIC intends to develop and implement its FISMA-compliant ISSP within FY04. The work breakdown on the following pages shows the planned schedule for completing the necessary tasks within this timeframe.

ID	Outline Nu	Task Name	Duration	Start	Finish	Predecessors
1	**1**	**Security Program Development**	**217 days**	**Mon 11/17/03**	**Wed 9/29/04**	
2						
3	**1.1**	**Preparation**	**40 days**	**Mon 11/17/03**	**Tue 1/20/04**	
4	**1.1.1**	**Research**	**10 days**	**Mon 11/17/03**	**Mon 12/1/03**	
5	1.1.1.1	Develop basic understanding of OPIC organization and business	10 days	Mon 11/17/03	Mon 12/1/03	
6	1.1.1.2	Develop basic understanding of OPIC IT environment	10 days	Mon 11/17/03	Mon 12/1/03	
7	1.1.1.3	Review existing OPIC IT and Security documentation	10 days	Mon 11/17/03	Mon 12/1/03	
8	1.1.1.4	Review relevant federal security requirements	10 days	Mon 11/17/03	Mon 12/1/03	
9	**1.1.2**	**System Documentation**	**30 days**	**Tue 12/2/03**	**Tue 1/20/04**	**4**
10	1.1.2.1	Identify Gaps in IT documentation	5 days	Tue 12/2/03	Mon 12/8/03	
11	1.1.2.2	Develop plan for filling gaps	5 days	Tue 12/9/03	Mon 12/15/03	10
12	1.1.2.3	Gather data as needed	10 days	Tue 12/16/03	Mon 1/5/04	11
13	1.1.2.4	Update/enhance documentation	10 days	Tue 1/6/04	Tue 1/20/04	12
14	1.1.2.5	Milestone: System Documentation Complete	0 days	Tue 1/20/04	Tue 1/20/04	13
15	**1.1.3**	**Planning**	**25 days**	**Mon 11/24/03**	**Mon 1/5/04**	
16	**1.1.3.1**	**Create plan for developing security program**	**10 days**	**Mon 11/24/03**	**Mon 12/8/03**	
17	1.1.3.1.1	Project schedule	5 days	Mon 11/24/03	Mon 12/1/03	
18	1.1.3.1.2	FISMA Program Plan	10 days	Mon 11/24/03	Mon 12/8/03	
19	1.1.3.2	Stakeholder review	10 days	Tue 12/9/03	Mon 12/22/03	16
20	1.1.3.3	Update as needed	5 days	Tue 12/23/03	Mon 1/5/04	19
21	1.1.3.4	Milestone: Security Program Planning Complete	0 days	Mon 1/5/04	Mon 1/5/04	20
22						
23	**1.2**	**Security Policies**	**38 days**	**Tue 1/6/04**	**Mon 3/1/04**	**15**
24	1.2.1	Create policy framework and templates	10 days	Tue 1/6/04	Tue 1/20/04	
25	1.2.2	Create list of policies	10 days	Tue 1/6/04	Tue 1/20/04	
26	1.2.3	Develop process for periodic review and update of policies	10 days	Tue 1/6/04	Tue 1/20/04	
27	**1.2.4**	**Policy Documentation**	**25 days**	**Wed 1/21/04**	**Wed 2/25/04**	**24,25,26**
28	1.2.4.1	Develop draft	10 days	Wed 1/21/04	Tue 2/3/04	
29	1.2.4.2	Peer review	3 days	Wed 2/4/04	Fri 2/6/04	28
30	1.2.4.3	update based on peer comments	2 days	Mon 2/9/04	Tue 2/10/04	29
31	1.2.4.4	Stakeholder review of policies	3 days	Wed 2/11/04	Fri 2/13/04	30
32	1.2.4.5	Update based on stakeholder comments	5 days	Tue 2/17/04	Mon 2/23/04	31
33	1.2.4.6	Gain agreement from stakeholders	2 days	Tue 2/24/04	Wed 2/25/04	32
34	1.2.5	Communicate policies	3 days	Thu 2/26/04	Mon 3/1/04	27
35	1.2.6	Milestone: Policy Development Complete	0 days	Mon 3/1/04	Mon 3/1/04	34
36						
37	**1.3**	**Security Awareness & Training**	**84 days**	**Thu 2/26/04**	**Wed 6/23/04**	**27**
38	1.3.1	Determine requirements	5 days	Thu 2/26/04	Wed 3/3/04	
39	1.3.2	Develop plan/framework	5 days	Thu 3/4/04	Wed 3/10/04	38
40	**1.3.3**	**Develop training**	**25 days**	**Thu 3/11/04**	**Wed 4/14/04**	**39**
41	1.3.3.1	Determine course outline	10 days	Thu 3/11/04	Wed 3/24/04	
42	1.3.3.2	Determine delivery method	10 days	Thu 3/11/04	Wed 3/24/04	
43	**1.3.3.3**	**Develop training materials**	**15 days**	**Thu 3/25/04**	**Wed 4/14/04**	**41,42**
44	1.3.3.3.1	Develop draft	10 days	Thu 3/25/04	Wed 4/7/04	
45	1.3.3.3.2	Peer review	3 days	Thu 4/8/04	Mon 4/12/04	44
46	1.3.3.3.3	Update based on peer comments	2 days	Tue 4/13/04	Wed 4/14/04	45
47	**1.3.4**	**Implement Training**	**19 days**	**Thu 4/15/04**	**Tue 5/11/04**	**40**
48	1.3.4.1	Prepare training environment (as needed)	3 days	Thu 4/15/04	Mon 4/19/04	
49	1.3.4.2	Conduct training for existing personnel	15 days	Tue 4/20/04	Mon 5/10/04	48
50	1.3.4.3	Update as needed based on training results	5 days	Tue 5/4/04	Mon 5/10/04	49FF
51	1.3.4.4	Incorporate training into new hire orientation	1 day	Tue 5/11/04	Tue 5/11/04	50
52	1.3.4.5	Milestone: Initial Security Training Complete	0 days	Tue 5/11/04	Tue 5/11/04	51
53	**1.3.5**	**Awareness campaign**	**30 days**	**Wed 5/12/04**	**Wed 6/23/04**	**47**
54	1.3.5.1	Determine delivery mechanisms	10 days	Wed 5/12/04	Tue 5/25/04	
55	1.3.5.2	Determine content	10 days	Wed 5/12/04	Tue 5/25/04	
56	1.3.5.3	Develop materials as needed	10 days	Wed 5/26/04	Wed 6/9/04	54,55
57	1.3.5.4	Review of content	3 days	Thu 6/10/04	Mon 6/14/04	56
58	1.3.5.5	Update as needed	2 days	Tue 6/15/04	Wed 6/16/04	57
59	1.3.5.6	Deliver content	5 days	Thu 6/17/04	Wed 6/23/04	58
60	1.3.5.7	Milestone: Security Awareness Program Initiated	0 days	Wed 6/23/04	Wed 6/23/04	59

ID	Outline Nui	Task Name	Duration	Start	Finish	Predecessors
61						
62	**1.4**	**Incident Management**	**70 days**	**Mon 2/2/04**	**Mon 5/10/04**	**15**
63	**1.4.1**	**Incident Reporting**	**30 days**	**Mon 2/2/04**	**Mon 3/15/04**	
64	1.4.1.1	Determine criteria for reporting	10 days	Mon 2/2/04	Fri 2/13/04	
65	1.4.1.2	Determine process for internal reporting of incidents	10 days	Mon 2/2/04	Fri 2/13/04	
66	1.4.1.3	Assign roles and responsibilities	10 days	Mon 2/2/04	Fri 2/13/04	
67	**1.4.1.4**	**Document process**	**20 days**	**Tue 2/17/04**	**Mon 3/15/04**	**64,66**
68	1.4.1.4.1	Develop draft	10 days	Tue 2/17/04	Mon 3/1/04	
69	1.4.1.4.2	Peer review	5 days	Tue 3/2/04	Mon 3/8/04	68
70	1.4.1.4.3	update based on comments	5 days	Tue 3/9/04	Mon 3/15/04	69
71	**1.4.2**	**Incident Response**	**25 days**	**Tue 3/2/04**	**Mon 4/5/04**	**68**
72	1.4.2.1	Determine procedures for response to incidents	10 days	Tue 3/2/04	Mon 3/15/04	
73	1.4.2.2	Assign roles and responsibilities	10 days	Tue 3/2/04	Mon 3/15/04	
74	1.4.2.3	Specify tools if needed	10 days	Tue 3/2/04	Mon 3/15/04	
75	**1.4.2.4**	**Document process**	**15 days**	**Tue 3/16/04**	**Mon 4/5/04**	**72,73,74**
76	1.4.2.4.1	Develop draft	10 days	Tue 3/16/04	Mon 3/29/04	
77	1.4.2.4.2	Peer review	3 days	Tue 3/30/04	Thu 4/1/04	76
78	1.4.2.4.3	update based on comments	2 days	Fri 4/2/04	Mon 4/5/04	77
79	**1.4.3**	**Stakeholder review**	**12 days**	**Tue 4/6/04**	**Wed 4/21/04**	**63,71**
80	1.4.3.1	Stakeholder review of procedures	5 days	Tue 4/6/04	Mon 4/12/04	
81	1.4.3.2	update based on stakeholder comments	5 days	Tue 4/13/04	Mon 4/19/04	80
82	1.4.3.3	gain stakeholder agreement	2 days	Tue 4/20/04	Wed 4/21/04	81
83	1.4.4	Implement incident reporting and response procedures	5 days	Thu 4/22/04	Wed 4/28/04	79
84	1.4.5	Communicate incident reporting and response procedures	5 days	Thu 4/22/04	Wed 4/28/04	79
85	1.4.6	Milestone: Internal Incident Reporting & Response Initiated	0 days	Wed 4/28/04	Wed 4/28/04	84,83
86	**1.4.7**	**Coordination with FedCirc**	**25 days**	**Tue 4/6/04**	**Mon 5/10/04**	**63,71**
87	1.4.7.1	Develop procedures for reporting to FedCirc	5 days	Tue 4/6/04	Mon 4/12/04	
88	1.4.7.2	Develop procedures for receiving and handling info from FedCirc	10 days	Tue 4/13/04	Mon 4/26/04	87
89	1.4.7.3	Communicate and implement FedCirc procedures	10 days	Tue 4/27/04	Mon 5/10/04	87,88
90	1.4.7.4	Finalize agreement	2 days	Fri 5/7/04	Mon 5/10/04	89FF
91	1.4.8	Milestone: FedCirc Incident Reporting Initiated	0 days	Mon 5/10/04	Mon 5/10/04	90
92						
93	**1.5**	**Risk Management**	**183 days**	**Tue 1/6/04**	**Thu 9/23/04**	
94	**1.5.1**	**Classification**	**42 days**	**Tue 1/6/04**	**Fri 3/5/04**	**15**
95	1.5.1.1	Develop framework for classification of system/data criticality	15 days	Tue 1/6/04	Tue 1/27/04	
96	1.5.1.2	Develop framework for classification of system/data sensitivity	15 days	Tue 1/6/04	Tue 1/27/04	
97	**1.5.1.3**	**Document classification criteria and procedures**	**27 days**	**Wed 1/28/04**	**Fri 3/5/04**	**95,96**
98	1.5.1.3.1	Develop draft	10 days	Wed 1/28/04	Tue 2/10/04	
99	1.5.1.3.2	Peer review	3 days	Wed 2/11/04	Fri 2/13/04	98
100	1.5.1.3.3	update based on peer comments	2 days	Tue 2/17/04	Wed 2/18/04	99
101	1.5.1.3.4	Stakeholder review of policies	5 days	Thu 2/19/04	Wed 2/25/04	100
102	1.5.1.3.5	Update based on stakeholder comments	5 days	Thu 2/26/04	Wed 3/3/04	101
103	1.5.1.3.6	Gain agreement from stakeholders	2 days	Thu 3/4/04	Fri 3/5/04	102
104	1.5.1.4	Milestone: Classification framework complete	0 days	Fri 3/5/04	Fri 3/5/04	97
105	**1.5.2**	**Risk Assessment**	**35 days**	**Tue 5/11/04**	**Tue 6/29/04**	**94,62**
106	1.5.2.1	Determine strategy for risk assessment	5 days	Tue 5/11/04	Mon 5/17/04	
107	1.5.2.2	Develop framework and templates	5 days	Tue 5/18/04	Mon 5/24/04	106
108	1.5.2.3	Implement tools as needed	20 days	Tue 5/25/04	Tue 6/22/04	107
109	1.5.2.4	Create & document procedures	10 days	Wed 6/9/04	Tue 6/22/04	108FF
110	1.5.2.5	Initiate periodic assessments	5 days	Wed 6/23/04	Tue 6/29/04	109
111	1.5.2.6	Milestone: Risk Assessment Framework Complete	0 days	Tue 6/29/04	Tue 6/29/04	110
112	**1.5.3**	**Vulnerability Testing**	**50 days**	**Tue 5/11/04**	**Wed 7/21/04**	**62**
113	1.5.3.1	Determine scope and objectives	5 days	Tue 5/11/04	Mon 5/17/04	
114	1.5.3.2	Develop plan for periodic testing	10 days	Tue 5/18/04	Tue 6/1/04	113
115	1.5.3.3	Select and acquire tools	10 days	Wed 6/2/04	Tue 6/15/04	114
116	1.5.3.4	Create testing procedures	10 days	Wed 6/16/04	Tue 6/29/04	115
117	1.5.3.5	implement testing	10 days	Wed 6/30/04	Wed 7/14/04	116
118	1.5.3.6	Optimize testing procedures	5 days	Thu 7/15/04	Wed 7/21/04	117
119	1.5.3.7	Milestone: Vulnerability Testing Initiated	0 days	Wed 7/21/04	Wed 7/21/04	118

ID	Outline Nui	Task Name	Duration	Start	Finish	Predecessors
120	**1.5.4**	**Certification & Accreditation**	**60 days**	**Wed 6/30/04**	**Thu 9/23/04**	**105**
121	1.5.4.1	Plan framework	15 days	Wed 6/30/04	Wed 7/21/04	
122	1.5.4.2	Develop Procedures	15 days	Wed 6/30/04	Wed 7/21/04	
123	1.5.4.3	Implement tools as needed	20 days	Thu 7/22/04	Wed 8/18/04	121
124	1.5.4.4	Create templates	5 days	Thu 7/22/04	Wed 7/28/04	121
125	1.5.4.5	Define and assign responsibilities	5 days	Thu 7/22/04	Wed 7/28/04	121
126	**1.5.4.6**	**Document C&A procedures**	**30 days**	**Thu 7/29/04**	**Thu 9/9/04**	**122,124,125**
127	1.5.4.6.1	Develop draft document	10 days	Thu 7/29/04	Wed 8/11/04	
128	1.5.4.6.2	peer review	2 days	Thu 8/12/04	Fri 8/13/04	127
129	1.5.4.6.3	update based on peer comments	3 days	Mon 8/16/04	Wed 8/18/04	128
130	1.5.4.6.4	Stakeholder review of document	5 days	Thu 8/19/04	Wed 8/25/04	129
131	1.5.4.6.5	update based on stakeholder comments	5 days	Thu 8/26/04	Wed 9/1/04	130
132	1.5.4.6.6	gain agreement on final	5 days	Thu 9/2/04	Thu 9/9/04	131
133	1.5.4.7	Milestone: C&A Program Initiated	0 days	Thu 9/9/04	Thu 9/9/04	126
134	1.5.4.8	Perform C&A of OPICNET	10 days	Fri 9/10/04	Thu 9/23/04	133
135	1.5.5	Incorporate risk management into system development lifecycle	30 days	Thu 8/12/04	Thu 9/23/04	133FF+10 days
136	1.5.6	Incorporate risk management into decision-making processes	30 days	Thu 8/12/04	Thu 9/23/04	133FF+10 days
137						
138	**1.6**	**OPICNET Security Plan**	**43 days**	**Mon 2/2/04**	**Thu 4/1/04**	**9**
139	1.6.1	Perform risk assessment on OPICNET	5 days	Mon 2/2/04	Fri 2/6/04	
140	1.6.2	Determine gaps in security controls	5 days	Mon 2/9/04	Fri 2/13/04	139
141	1.6.3	Create plan for addressing gaps	5 days	Tue 2/17/04	Mon 2/23/04	140
142	**1.6.4**	**Documentation**	**28 days**	**Tue 2/24/04**	**Thu 4/1/04**	**141**
143	1.6.4.1	Develop draft security plan	10 days	Tue 2/24/04	Mon 3/8/04	
144	1.6.4.2	peer review	3 days	Tue 3/9/04	Thu 3/11/04	143
145	1.6.4.3	update based on peer comments	5 days	Fri 3/12/04	Thu 3/18/04	144
146	1.6.4.4	stakeholder review	5 days	Fri 3/19/04	Thu 3/25/04	145
147	1.6.4.5	update based on stakeholder comments	3 days	Fri 3/26/04	Tue 3/30/04	146
148	1.6.4.6	obtain stakeholder agreement	2 days	Wed 3/31/04	Thu 4/1/04	147
149	1.6.5	Milestone: OPICNET Security Plan complete	0 days	Mon 2/2/04	Mon 2/2/04	
150						
151	**1.7**	**Continuity of Operations/Disaster Recovery**	**127 days**	**Thu 4/1/04**	**Wed 9/29/04**	**9**
152	1.7.1	Review existing DRP/COOP	10 days	Thu 4/1/04	Wed 4/14/04	
153	1.7.2	Identify Gaps	10 days	Thu 4/1/04	Wed 4/14/04	
154	1.7.3	Identify key stakeholders and points of contact	10 days	Thu 4/1/04	Wed 4/14/04	
155	1.7.4	Interview key stakeholders	10 days	Thu 4/15/04	Wed 4/28/04	154,153
156	**1.7.5**	**Determine requirements**	**15 days**	**Thu 4/29/04**	**Wed 5/19/04**	**155**
157	1.7.5.1	Document disaster recovery/business continuity priorities	5 days	Thu 4/29/04	Wed 5/5/04	
158	1.7.5.2	stakeholder review	5 days	Thu 5/6/04	Wed 5/12/04	157
159	1.7.5.3	update based on stakeholder comments	3 days	Thu 5/13/04	Mon 5/17/04	158
160	1.7.5.4	gain agreement on final	2 days	Tue 5/18/04	Wed 5/19/04	159
161	**1.7.6**	**Develop plan**	**35 days**	**Thu 5/20/04**	**Fri 7/9/04**	**156**
162	1.7.6.1	Develop draft document	15 days	Thu 5/20/04	Thu 6/10/04	
163	1.7.6.2	peer review	2 days	Fri 6/11/04	Mon 6/14/04	162
164	1.7.6.3	update based on peer comments	3 days	Tue 6/15/04	Thu 6/17/04	163
165	1.7.6.4	Stakeholder review of document	5 days	Fri 6/18/04	Thu 6/24/04	164
166	1.7.6.5	update based on stakeholder comments	5 days	Fri 6/25/04	Thu 7/1/04	165
167	1.7.6.6	gain agreement on final	5 days	Fri 7/2/04	Fri 7/9/04	166
168	1.7.7	Milestone: Disaster Recovery Plan Updated	0 days	Fri 7/9/04	Fri 7/9/04	161
169	**1.7.8**	**Testing**	**37 days**	**Mon 7/12/04**	**Tue 8/31/04**	**161**
170	1.7.8.1	Plan test	10 days	Mon 7/12/04	Fri 7/23/04	
171	1.7.8.2	Prepare for test	15 days	Mon 7/26/04	Fri 8/13/04	170
172	1.7.8.3	Perform test	2 days	Mon 8/16/04	Tue 8/17/04	171
173	1.7.8.4	Document test results	10 days	Wed 8/18/04	Tue 8/31/04	172
174	1.7.8.5	Milestone: Disaster Recovery Plan Tested	0 days	Tue 8/31/04	Tue 8/31/04	173
175	**1.7.9**	**Optimize**	**15 days**	**Wed 9/1/04**	**Wed 9/22/04**	**169**
176	1.7.9.1	Analyze test results	5 days	Wed 9/1/04	Wed 9/8/04	
177	1.7.9.2	Update plan as needed	10 days	Thu 9/9/04	Wed 9/22/04	176
178	1.7.10	Develop and implement plan for periodic update and testing of DRP/COOP	5 days	Thu 9/23/04	Wed 9/29/04	175
179	1.7.11	Milestone: Disaster Recovery Program Complete	0 days	Wed 9/29/04	Wed 9/29/04	178

ID	Outline Nui	Task Name	Duration	Start	Finish	Predecessors
180						
181	**1.8**	**Resolve Vulnerability Findings**	**53 days**	**Mon 2/9/04**	**Thu 4/22/04**	**138SS**
182	**1.8.1**	**Determine strategy for addressing vulnerabilities**	**15 days**	**Mon 2/9/04**	**Mon 3/1/04**	
183	1.8.1.1	Server and workstation standards	10 days	Wed 2/11/04	Wed 2/25/04	27FF
184	1.8.1.2	Hardening of servers and network devices	10 days	Wed 2/11/04	Wed 2/25/04	27FF
185	1.8.1.3	Patches and security updates	10 days	Wed 2/11/04	Wed 2/25/04	27FF
186	1.8.1.4	Authentication issues	15 days	Mon 2/9/04	Mon 3/1/04	27FF
187	**1.8.2**	**Develop technical implementation plan**	**18 days**	**Tue 3/2/04**	**Thu 3/25/04**	**182**
188	1.8.2.1	Draft	10 days	Tue 3/2/04	Mon 3/15/04	
189	1.8.2.2	Peer review	3 days	Tue 3/16/04	Thu 3/18/04	188
190	1.8.2.3	update as needed	5 days	Fri 3/19/04	Thu 3/25/04	189
191	1.8.3	implement plan	20 days	Fri 3/26/04	Thu 4/22/04	187
192	1.8.4	document actions completed	10 days	Fri 4/9/04	Thu 4/22/04	191FF
193	1.8.5	Milestone: Vulnerability Findings Resolved	0 days	Thu 4/22/04	Thu 4/22/04	192
194						
195	**1.9**	**Implement Security Measures**	**176 days**	**Mon 1/5/04**	**Mon 9/13/04**	
196	**1.9.1**	**Virus Management**	**30 days**	**Mon 1/5/04**	**Tue 2/17/04**	
197	1.9.1.1	Develop technical plan	10 days	Mon 1/5/04	Fri 1/16/04	
198	1.9.1.2	Implement Plan	20 days	Tue 1/20/04	Tue 2/17/04	197
199	1.9.1.3	Milestone: Enhanced Virus Management Implemented	0 days	Tue 2/17/04	Tue 2/17/04	198
200	**1.9.2**	**Password management**	**10 days**	**Mon 1/5/04**	**Fri 1/16/04**	
201	1.9.2.1	Develop technical plan	5 days	Mon 1/5/04	Fri 1/9/04	
202	1.9.2.2	Implement Plan	5 days	Mon 1/12/04	Fri 1/16/04	201
203	1.9.2.3	Milestone: Password Management Implemented	0 days	Fri 1/16/04	Fri 1/16/04	202
204	**1.9.3**	**Audit trails**	**30 days**	**Tue 2/17/04**	**Mon 3/29/04**	
205	1.9.3.1	Develop technical plan	10 days	Tue 2/17/04	Mon 3/1/04	
206	1.9.3.2	Implement Plan	20 days	Tue 3/2/04	Mon 3/29/04	205
207	1.9.3.3	Milestone: Audit Trails Implemented	0 days	Mon 3/29/04	Mon 3/29/04	206
208	**1.9.4**	**Identification and Authentication**	**53 days**	**Mon 2/23/04**	**Wed 5/5/04**	**196**
209	1.9.4.1	Develop technical plan	15 days	Mon 2/23/04	Fri 3/12/04	
210	1.9.4.2	Implement Plan	30 days	Thu 3/25/04	Wed 5/5/04	209
211	1.9.4.3	Milestone: Enhanced Identification and Authentication Implemented	0 days	Wed 5/5/04	Wed 5/5/04	210
212	**1.9.5**	**Logical Controls over network access**	**30 days**	**Thu 5/6/04**	**Thu 6/17/04**	**208**
213	1.9.5.1	Develop technical plan	10 days	Thu 5/6/04	Wed 5/19/04	
214	1.9.5.2	Implement Plan	20 days	Thu 5/20/04	Thu 6/17/04	213
215	1.9.5.3	Milestone: Enhanced Logical Access Controls Implemented	0 days	Thu 6/17/04	Thu 6/17/04	214
216	**1.9.6**	**Mobile Computing protections**	**30 days**	**Thu 5/6/04**	**Thu 6/17/04**	**208**
217	1.9.6.1	Develop technical plan	10 days	Thu 5/6/04	Wed 5/19/04	
218	1.9.6.2	implement plan	20 days	Thu 5/20/04	Thu 6/17/04	217
219	1.9.6.3	Milestone: Mobile Computing Protections Implemented	0 days	Thu 6/17/04	Thu 6/17/04	218
220	**1.9.7**	**Personnel Controls**	**60 days**	**Thu 5/6/04**	**Fri 7/30/04**	
221	**1.9.7.1**	**Background screening**	**30 days**	**Fri 6/18/04**	**Fri 7/30/04**	**216**
222	1.9.7.1.1	Develop technical plan	10 days	Fri 6/18/04	Thu 7/1/04	
223	1.9.7.1.2	implement plan	20 days	Fri 7/2/04	Fri 7/30/04	222
224	1.9.7.1.3	Milestone: IT Background Screening Implemented Implemented	0 days	Fri 7/30/04	Fri 7/30/04	223
225	**1.9.7.2**	**separation of duties**	**30 days**	**Thu 5/6/04**	**Thu 6/17/04**	**208**
226	1.9.7.2.1	Develop technical plan	10 days	Thu 5/6/04	Wed 5/19/04	
227	1.9.7.2.2	implement plan	20 days	Thu 5/20/04	Thu 6/17/04	226
228	1.9.7.2.3	Milestone: IT Separation of Duties Implemented	0 days	Thu 6/17/04	Thu 6/17/04	227
229	**1.9.7.3**	**least priviledge**	**30 days**	**Fri 6/18/04**	**Fri 7/30/04**	**212**
230	1.9.7.3.1	Develop technical plan	10 days	Fri 6/18/04	Thu 7/1/04	
231	1.9.7.3.2	implement plan	20 days	Fri 7/2/04	Fri 7/30/04	230
232	1.9.7.3.3	Milestone: Least Privilege Implemented	0 days	Fri 7/30/04	Fri 7/30/04	231
233	**1.9.8**	**Media Management**	**30 days**	**Mon 8/2/04**	**Mon 9/13/04**	**221**
234	1.9.8.1	Develop policies and procedures	10 days	Mon 8/2/04	Fri 8/13/04	
235	1.9.8.2	Implement policies and procedures	20 days	Mon 8/16/04	Mon 9/13/04	234
236	1.9.8.3	Milestone: Media Management Implemented	0 days	Mon 9/13/04	Mon 9/13/04	235
237	**1.9.9**	**Data Integrity & Validation**	**30 days**	**Mon 8/2/04**	**Mon 9/13/04**	**229**
238	1.9.9.1	Develop policies and procedures	10 days	Mon 8/2/04	Fri 8/13/04	
239	1.9.9.2	Implement policies and procedures	20 days	Mon 8/16/04	Mon 9/13/04	238
240	1.9.9.3	Milestone: Data Integrity & Validation Implemented	0 days	Mon 9/13/04	Mon 9/13/04	239