Global Information Assurance Certification Paper

System Security Plan Auditing For System Owners

Michael Kirby
CISSP, GSEC, GGSC

November 2003

Introduction

The objective of system and site security planning is to improve protection of information technology (IT) resources. All systems and sites have some level of sensitivity and require protection as part of good management practices. The level of sensitivity should at least be ***Sensitive But Unclassified***. All aspects of protection of a system or site must be clearly documented in this system security plan. The completion of these plans is a requirement established by Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," Public Law 100-235, "Computer Security Act of 1987.

The System Owner is responsible for ensuring that the system security plan is prepared and for implementing the plan and monitoring its effectiveness. System security plans should reflect input from various individuals with responsibilities concerning the system, including functional "end users," Information Owners, the System Administrator, and the System Security Manager.

System Security Plan

The purpose of the security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. It should reflect input from various managers with responsibilities concerning the system, including information owners, the system operator, and the system security manager. Additional information may be included in the basic plan and the structure and format organized according to agency needs, so long as the major sections described in this document are adequately covered and readily identifiable.

Overview of security requirements for a system

The Computer Security Act of 1987 mandated that federal agencies authorize systems prior to deploying them. OMB A-130 requires that System Owners ensure the development of System Security Plans and Contingency Plans and that self-assessments are performed to identify vulnerabilities and that appropriate corrective action is taken. It also requires that the federal agency's IT assets be authorized to operate. Certification and Accreditation activities lead to that authorization.

The Certification and Accreditation (C&A) Process consists of four Phases:

- Phase 1, Pre-certification focuses on understanding the mission, environment, and architecture; defining security requirements necessary to achieve accreditation; and making an initial risk assessment. The objective of Phase 1 is to reach agreement between the Accreditation Manager, Certifying Agent, System Owner and other C&A Team members on the security requirements, certification level, and resources required for C&A. At this point all necessary documentation is collected.

- Phase 2, Certification - also known as Verification - validates the evolving or modified system's compliance with the information contained in the **System Security Plan (SSP)**. The SSP is the driving document for Phase 2 of the C&A process.

- Phase 3, Accreditation, produces the required evidence to support the Designated Approving Authority (DAA) in making an informed decision about granting authorization to operate the system. The risk assessment report is the driving document for Phase 3.

- Phase 4, Post-Accreditation, includes those activities necessary to adhere to the system's accredited security posture. Major modifications to the system or significant changes in threats or environment initiate a new C&A cycle. Otherwise the system must undergo C&A every three years.

Controls to meet those requirements

Below are the minimum-security controls that must be in place prior to authorizing a system for processing. The level of controls should be consistent with the level of sensitivity the system contains.

- Technical and/or security evaluation complete.
- Risk assessment conducted.
- Rules of behavior established and signed by users.
- Contingency plan developed and tested.
- **Security plan developed, updated, and reviewed.**
- System meets all applicable federal laws, regulations, policies, guidelines, and standards.
- In-place and planned security safeguards appear to be adequate and appropriate for the system.

Delineate responsibilities and behavior of individuals

Both the security official and the authorizing management official have security responsibilities. The security official is closer to the day-to-day operation of the system and will direct, perform, or monitor security tasks. The authorizing official will normally have general responsibility for the organization supported by the system. Authorization is not a decision that should be made by the security staff. Formalization of the system authorization process reduces the potential that systems will be placed into a production environment without appropriate management review.

Management authorization must be based on an assessment of management, operational, and technical controls. The authorization must be supported by a technical/security evaluation called the Certification Report prepared by the Certifying agent. The security plan establishes the system protection requirements and documents the security controls in the system, it should help support the certification effort. Re-authorization should occur prior to a significant change in the system, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

Director

The Director is responsible for oversight to ensure an adequate level of protection is afforded, through an appropriate mix of technical, administrative, and managerial controls. The Director oversees the development of policies and procedures, ensures the development and presentation of user and contractor awareness sessions, inspects and spot checks to determine that an adequate level of compliance with security requirement exists. The Director is responsible for ensuring periodic vulnerability analyses to help determine if security controls are adequate. Special attention will be given to those new and developing technologies, systems and applications that can open or have opened vulnerabilities in the system's security posture.

Information Systems Security Officer (ISSO)

The ISSO is the focal point for information systems security concerns and ensures that the program requirements are implemented. The ISSO must possess knowledge of the organization's mission, mission information sensitivity, and information technology to ensure that the program requirements are met. The ISSO implements the overall information system security program for an organization and should not participate in daily information system operations. An ISSO may be appointed for each major information system or group of information systems that support the mission. The ISSO acts on behalf of the organization to ensure compliance with the information system security procedures. The same ISSO may be appointed for multiple information systems, local area networks, or small systems or workstations that provide automated technical security controls for individual accountability, access control, and auditing. "ISSO" does not necessarily refer to the specific functions of a single individual. Technical managers who are assigned as an ISSO will be provided sufficient information security training to effectively administer the information systems under their cognizance. The ISSO is responsible to the system owner or Certifying Authority for maintaining the approved accredited baseline.

System Managers and Administrators

System administrative staff maintains the system and user accounts, perform system backups, administers access control lists, manage the operating system/changes, etc. They have the same security responsibilities of users, but their responsibilities are expanded to recognize their *privileged user* status. System administrators must restrict themselves from using their position to turn off/destroy audit trails, not to give unauthorized individuals privileged access, and not to modify the system to negate automated security mechanisms.

System Technicians

System technicians (programmers, developers, and integrators) are responsible for acquiring, developing or integrating information systems that ensure systems security. System developers shall ensure that the requirements outlined in this instruction, and the specific requirements established by the functional application, are incorporated into the systems during the development process. System developers will designate responsible individuals to oversee the security aspects of the acquisition, development, and integration of the information system.

Users

Users are individuals who access an automated system either by direct connections or indirect connections (obtain system outputs without having to directly access the system). Users must report security problems, be alert for viruses, protect their access token, and, through their supervisor, ensure the ISSO is notified if access is no longer required.

Assignment 1: Research in Audit, Measurement, Practice and Control

Government wide Laws and Regulations

The following laws and regulations affect the System Security Plan. The Office of Management and Budget has mandated the System Security Plan and highly recommends utilizing NIST 800-18 guidance.

OMB Circular A-130, Appendix III

Establishes policy for the management of Federal information resources as well as procedures for information system security.

Computer Security Act, 1987

Requires all users of automated information systems owned or operated by the federal government receive specific training and education with respect to their roles and responsibilities in safeguarding systems and information processed, stored, or transmitted on such systems. This is the first Law passed that required System Security Plans for all systems,

GISRA Government Information Security Reform Act

Congress passed into law, GISRA, in the year 2000; its sunset was in the year 2002. It required government agencies to report their security posture. This Law required that agencies report the following to the Office of Management and Budget:

- Accreditation status of all systems
- Does the agency have a system security plan for all major systems
- Does the agency have a contingency plan for all systems

Many agencies were not committed to these requirements due to the limited sunset on this. Thus congress passed a new law:

FISMA Federal Information Security Management Act

Congress liked the GISMA so much that upon its sunset it passed into law FISMA, requiring all agencies to report their security posture as an ongoing cycle. At this point OMB started withholding money for new systems and upgrades until the agencies security posture was established for all systems

NIST 800-18 Guide for Developing Security Plans for Information Technology Systems

NIST 800-18 is the core of the System Security Plan. The System Security Plan for sites was derived from this document. Utilizing the outline of a SSP from this document created the basic checklist for an

audit of a SSP. Additionally all questions were derived from the basic needs from each section of the NIST 800-18 explanations of the SSP.

Types of Systems

Federal guidance for security plans (OMB Bulletin No. A-130, Appendix III) establishes two System categories: Major Application and General Support System. The target system should meet the criteria for a Major Application or General Support system. These systems have defined functions and readily identifiable security needs.

All applications and systems must be covered by system security plans if they are categorized as a "major application" or "general support system." Specific security plans for other applications are not required because the security controls for those applications or systems would be provided by the general support systems in which they operate. For example, a department-wide Financial Management System would be a major application requiring its own security plan. A local program designed to track expenditures against an office budget might not be considered a major application and would be covered by a general support system security plan for an office automation system or a local area network (LAN). Standard commercial off-the-shelf software (such as word processing software, electronic mail software, utility software, or other general- purpose software) would not typically be considered a major application and would be covered by the plans for the general support system on which they are installed.

Major Application

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

General Support Systems

General Support System is 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/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Four Areas of a System Security Plan

Identification

The first section of the plan provides basic identifying information about the system. Both types of plans must contain general descriptive information regarding who is responsible for the system, the purpose of the system, and the **sensitivity** of the system.

Management Control Area

In this section, the System Security Plan describes the management control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application or general support system. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system.

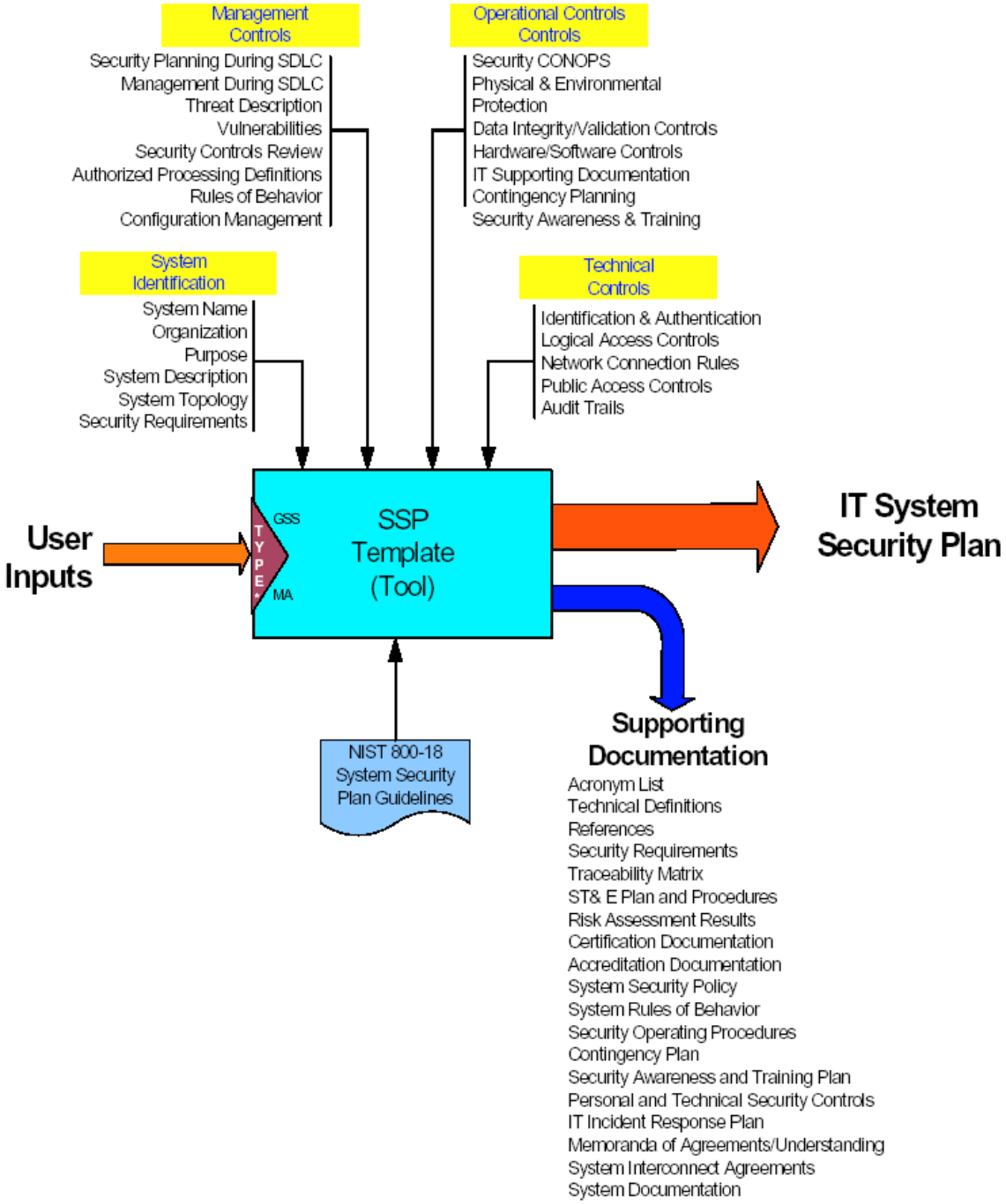
Operation Control Areas

The operational controls address security methods that focus on mechanisms that primarily 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). They often require technical or specialized expertise – and often rely upon management activities as well as technical controls. In this section, describe the operational control measures (in place or planned) that are intended to meet the protection requirements of the target systems

Technical Control Areas

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. In this section, describe the technical control measures (**in place** or **planned**) that are intended to meet the protection requirements of the major application or general support system.

System Security Plan Schematic



We will now create a checklist based on the above requirements.

Assignment 2: Create an Audit Checklist

The following tables were created based on the NIST 800-18 guidelines. They will address the SSP in the General Support System context. They consist of the following fields:

- Description – This information is based on the NIST 800- 18 Outline of a System Security Plan
- Yes – Enter a checkmark here if the plan has met the requirements in the notes column
- No – Enter a checkmark here if the plan does not meet the requirements in the notes column
- N/A – Enter a checkmark here if this part of the SSP is not applicable to the system being audited
- Notes – Information of what should be in the SSP in this part of the outline (includes NIST 800-18 section reference)
- Level - The column Level refers to the importance of this portion of the document. There are three levels:
    - L Low Not important but may be added
    - M Medium Important to the document
    - H High Necessary to the integrity of the document

Note: The three levels translate over to a risk management system also described by NIST.

Audit Checklist

System Identification

Description	Yes	No	N\A	Notes	Level
System Name / Title				Name given to the system (should be unique) NIST 800-18 3.2.1	H
Responsible Organization				List organization responsible for the system, and its location NIST 800-18 3.2.2	H
Information Contacts				Who is/are the point(s) of contact(s)? Need name, title, organization, and phone numbers – office, home and mobile if available. Should be more than one person – System Owner, System Manager, Project Manager, etc. NIST 800-18 3.2.3	L
Assignment of Security Responsibilities				Who is responsible for the security of the system – e.g. ISSO and alternate ISSO – you need the name, title, organization and phone numbers? NIST 800-18 3.2.4	H
System Operational Status				Operational status (i.e. Operational, Under Development, Undergoing a major modification)? NIST 800-18 3.3	M
General Description / Purpose				Does the security plan General Description / Purpose section describe? • The function or purpose of the system and the information processed. Is it a Major Application or General Support System? • The processing flow of the application from system input to system output. • The user organizations (internal and external) and type of data and processing provided. • Are the applications supported by the general support system listed? NIST 800-18 3.4	H
System Environment				Does the security plan include a System Environment section? • Provides a general description of the technical system (include a topology diagram as appropriate) • Provides a description of the primary computing platform(s) • Includes any security software protecting the system and information. NIST 800-18 3.5	M

System Identification (Continued)

Description	Yes	No	N\A	Notes	Level
System Interconnection				Does the system support interconnection / information sharing? Are system applications included as part of the sub-network via remote sites? • List of interconnected systems and system identifiers (if appropriate). • If connected to an external system not covered by a security plan, provides a short discussion of any security concerns that need to be considered for protection. • The authorization document should detail the rules of behavior that must be maintained by the interconnecting systems. Include copies of an existing agreements and Memorandums of Agreement. NIST 800-18 3.6	M
Information Classification				What is the sensitivity and criticality of the information stored within, processed by, or transmitted? (e.g. Sensitive but Unclassified or Classified – Secret high) NIST 800-18 3.7	H
Applicable Laws and Regulations				Includes a list of applicable laws and regulations that affect the system. Lists any laws or regulations that establish specific requirements for confidentiality, integrity, or availability of data/information in the system. NIST 800-18 3.7.1	L
General Description of Information Sensitivity				Does general description include the following: • Describes, in general terms, the information handled by the system and the need for protective measures. Relates the information handled to each of the three basic protection requirements (confidentiality, integrity, and availability). For each of the three categories, indicates if the requirement is: High, Medium, or Low. • Include a statement of the estimated risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information in the system. NIST 800-18 3.7.2	L

Management Controls

Description	Yes	No	N/A	Criteria	Level
Risk Assessment				• Has a risk assessment been conducted on the system? • Indicates who (security personnel) will be responsible for the periodic system reviews? • Does the security plan reference the risk assessment methodology used to identify the threats and vulnerabilities? NIST 800-18 4.1	M
Adequate Cost Effective Security				Does the risk assessment methodology used, provide an adequate cost effective security?	L
Factors:					
Value				Does it address the value of the information and systems contained?	M
Threat				Are the threats adequately described in the risk assessment?	M
Vulnerabilities				Are the vulnerabilities completely identified?	M
Effectiveness				Is the methodology used effective?	M
Review of Security Controls				When was the most recent audit/review? Gives the audit report number and the names of the team members and the date of the (expected, if applicable) completion date for this report. NIST 800-18 4.2	M
OMB A-130					
Annual Self Assessments				Are self-assessments done annually? Is it notated with the last date and the person performing it?	M
Rules of Behavior				Does the security plan provide Rules Of Behavior (ROB)? – May be placed in an appendix. • Does the ROB limit interconnections to other systems? • Does ROB define service provision and restoration priorities? • Does the ROB include a statement and signature and date line that user acknowledges receipt, understands responsibilities and will comply with the rules? • Are ROB signature pages kept on file for all users? NIST 800-18 4.3	H
Scope of Responsibilities				Does the ROB clearly delineate responsibilities and expected behavior of all individuals with access to the system?	H

Management Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Consequences				Is the ROB clear about the consequences of behavior that is not consistent with the rules?	M
Unofficial use of Government Computers				Does the ROB clearly delineate the rules for unofficial use of Government Computers pertinent to the agency involved?	L
Planning for Security in the Life Cycle				Is there a plan for security in the Life cycle that includes: • Does the security plan state the system's life cycle phase? • Does the security plan describe the security activities required in this Operation / Maintenance phase • Does security plan describe how information is moved, archived, discarded, or destroyed? NIST 800-18 4.4	M
Authorized Processing				Has the network system been approved for processing – if so, gives the name and title of the approving individual and the authorization date? NIST 800-18 4.5	M

Operational Controls

Description	Yes	No	N/A	Criteria	Level
Personnel Security				Does the personnel security section include: NIST 800-18 5.GSS.1	M
Background Investigation				• Does the security plan confirm all positions been reviewed for sensitivity level? • Does the security plan confirm user received background screenings appropriate for the position?	M
Least Privilege				Does the security plan confirm user access is restricted to the minimum necessary to perform the job?	L
Separation of Duties				Does the security plan confirm the implementation of separation of duties? (A matrix with position categories (roles) and associated access level is suggested)	L
User Accounts				Is there a process for requesting, establishing, issuing, and closing user accounts?	H
User Responsibility				Does the System Security Plan clearly state the Users responsibility regarding security? • Password policy • Logging off • Software installs	L
Termination Procedures				Does the security plan describe friendly and unfriendly termination procedures?	H
Physical and Environmental Protection				Does the security plan describe the following physical and environmental protections in the processing area? • Physical access • Fire safety • Utilities failure, water damage • Data intercept • Mobile and portable systems NIST 800-18 5.GSS.2	M
Production Input \ Output Controls				Does the security plan describe the following controls for input and output information and media? • Marking • Handling • Processing • Storage and disposal Does the security plan identify controls used to monitor the installation, and updates to software NIST 800-18 5.GSS.3	M

Operational Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Contingency Planning				Are there written procedures that document access controls, emergency procedures in event of natural or other disaster, and physical security precautions. NIST 800-18 5.GSS.4	H
Application Software and Hardware Maintenance Controls				Are the following Hardware and System Software Maintenance Controls addressed in the plan? • Maintenance and repair (including emergencies) • Items serviced through on-site and off-site • Version control • Testing and/or approving system components. • Impact analyses • Change identification • Documentation updates. • Use of test data • Policies against illegal use of copyrighted materials NIST 800-18 5.GSS.5	L
Data Integrity / Validation Controls				Are the following integrity controls addressed? • Virus detection and elimination • Integrity verification • Are intrusion detection tools installed on the system? • Performance monitoring • Message authentication • Reconciliation • Malicious Programs NIST 800-18 5.GSS.6	M

Operational Controls (Continued)

Documentation				Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to Automated Information System security in the application and the support systems(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures. List the documentation maintained for the application: • Hardware/software • Functional requirements • Security plan • General system security plan • Application program manuals • Test results documents • Standard operating procedures • Emergency procedures • Contingency plans • User rules/procedures • Risk assessment • Certification/accreditation statements/documents • Verification reviews/site inspections NIST 800-18 5.GSS.7	M
Hardware / Software Policies				Are there any in-house developed software associated with or used by the system and did it follow the established guidelines for software development lifecycle?	H
Standards:					
Procedures				Is there a configuration management program that includes reviewing, testing, and documenting modifications?	M
Approvals				Which group is responsible for controlling licensing and distribution of the software?	M
Backup Plan				Does the Security Plan include a description of the Backup Plan to include: • Frequency • Off site storage • Testing • Hardware/software information	H
Contingency Plans				Has a Contingency Plan been completed? If so, a copy should be included with the SSP.	H

Operational Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Security Awareness and Training				• Is there a security awareness-training program? • Does the security plan describe the security awareness & training program for the system? • Does the security awareness and training program cover the Rules of Behavior? NIST 800-18 5.GSS.8	M
Incident Response Capability				• Does the security plan describe procedures for reporting and handling incidents? • Does the security plan describe how alerts/advisories and response are handled? • Does the security plan define preventative measures that are in place to prevent intrusions? NIST 800-18 5.GSS.9	H

Technical Controls

Description	Yes	No	N/A	Criteria	Level
Identification and Authentication				Are there technical controls regarding user identification (e.g. first initial of the first name together with the full last name –max. of eight (8) characters) and authentication (password) procedures? List the requirements associated with passwords? NIST 800-18 6.GSS.1	H
Logical Access Control				Does the security plan describe how access rights are granted? Are the following controls described in the plan? • Restricting to system resources not needed in the performance of job. • Controls to detect unauthorized transaction • Time out controls related to periods of user inactivity. • The use of warning banners. NIST 800-18 6.GSS.2	H
Public Access Control				Public Access Controls (MA Only) - If the public accesses the major application, discuss the additional security controls used to protect the integrity of the application and the confidence of the public in the application. Such controls include segregating information made directly accessible to the public from official agency records. Others might include: • Some form of identification and authentication • Access control to limit what the user can read, write, modify, or delete • Controls to prevent public users from modifying information on the system • Digital signatures • CD-ROM for on-line storage of information for distribution • Put copies of information for public access on a separate system • Prohibit public to access live databases • Verify that programs and information distributed to the public are virus-free • Audit trails and user confidentiality • System and data availability • Legal considerations	H

Technical Controls (continued)

Compensating Controls Provided				Audit Trails? • Does the audit trail support accountability by providing a trace of user actions? • Are audit trails designed and implemented to record appropriate information that can assist in intrusion detection? • Does the audit trail include sufficient information to establish what events occurred and who (or what) caused them? (Type of event, when the event occurred, user id associated with the event, program or command used to initiate the event.) • Is access to online audit logs strictly enforced? • Is the confidentiality of audit trail information protected if, for example, it records personal information about users? • Describe how frequently audit trails are reviewed and whether there are guidelines. • Does the appropriate system-level or application-level administrator review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem • Does the ISSO review audit trail/logs (at least monthly) NIST 800-18 6.GSS.3	M

Assignment 3: Audit Report

The objective of this task is to characterize all vulnerabilities identified in the SSP Checklist report to determine whether the risks require remediation or acceptance. The checklist activities, through a series of verification techniques and procedures, should demonstrate which of the needed security controls are correctly implemented and effective in their application. Partial implementation and/or missing security controls also are identified during the checklist phase. The Certifier's audit Report is the product of the analysis of the checklist findings.

The checklist below was applied to the sample System Security Plan in Appendix C and should be attached to the final report.

Audit Checklist

System Identification

Description	Yes	No	N\A	Comments	Level
System Name / Title	X				H
Responsible Organization	X				H
Information Contacts	X				L
Assignment of Security Responsibilities	X				H
System Operational Status	X				M
General Description / Purpose	X				H
System Environment		X		Meets all requirements except a topology diagram is not attached. Recommend creating a topology diagram	M

System Identification (Continued)

Description	Yes	No	N\A	Comments	Level
System Interconnection	X				M
Information Classification	X				H
Applicable Laws and Regulations	X				L
General Description of Information Sensitivity	X				L

Management Controls

Description	Yes	No	N/A	Comment	Level
Risk Assessment		X		A risk assessment has not been done on this system	M
Adequate Cost Effective Security	X				L
Factors:					
Value		X		It does not address the value of the information and systems contained.	M
Threat		X		The threats are not adequately described in the risk assessment.	M
Vulnerabilities		X		The vulnerabilities are not identified.	M
Effectiveness	X				M
Review of Security Controls	X				M
OMB A-130					
Annual Self Assessments	X				M
Rules of Behavior	X			Does the security plan provide rules of behavior (ROB)? – May be placed in an appendix. • Does the ROB limit interconnections to other systems? • Does ROB define service provision and restoration priorities? • Does the ROB include a statement and signature and date line that user acknowledges receipt, understands responsibilities and will comply with the rules? • Are ROB signature pages kept on file for all users?	H
Scope of Responsibilities		X		Needs to be defined and documented	H

Management Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Consequences	X				M
Unofficial use of Government Computers	X				L
Planning for Security in the Life Cycle		X		Needs information on how media is moved, destroyed etc.	M
Authorized Processing		X		Needs to have C&A done	M

Operational Controls

Description	Yes	No	N/A	Criteria	Level
Personnel Security				Does the personnel security section include:	
Background Investigation	X				M
Least Privilege		X		This needs to be implemented and documented.	L
Separation of Duties		X		This needs to be implemented and documented.	L
User Accounts		X		This needs to be implemented and documented.	H
User Responsibility	X				L
Termination Procedures		X		This needs to be implemented and documented.	H
Physical and Environmental Protection	X			This is marked yes, but the documentation should be expanded on.	M
Production Input \ Output Controls		X		This needs to be implemented and documented.	M

Operational Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Contingency Planning		X		Need to attach contingency plan	H
Application Software and Hardware Maintenance Controls	X				L
Data Integrity / Validation Controls	X				M

Operational Controls (Continued)

Documentation	X				M
Hardware / Software Policies	X				H
Standards:					
Procedures	X				M
Approvals	X				M
Backup Plan		X		This needs to be implemented and documented.	H
Contingency Plans	X			Copy not available	H

Operational Controls (Continued)

Description	Yes	No	N/A	Criteria	Level
Security Awareness and Training		X		Needs to flesh out Security and Awareness training	M
Incident Response Capability	X				H

Technical Controls

Description	Yes	No	N/A	Criteria	Level
Identification and Authentication	X			.	H
Logical Access Control	X				H
Public Access Control			X	Not necessary, this is a GSS.	H
Compensating Controls Provided	X				M

Final Report

Summary

Overall this is a good System Security Plan. Its basic fundamentals are included. With a few additions, the SSP will be able to pass an Inspector General's Audit. Below listed by Level (criticality) are the recommendations for improvement.

Level – High should be done as soon as possible

- Scope of responsibilities – in the Rules of behavior responsibilities of the owner, system manager, user etc. needs to be defined. Some examples of responsibilities may include the owner has the overall security responsibility for the system, and the system manager has technical responsibility for the system. NIST 800-18 4.3
- User Accounts – the process for creating user accounts needs to be created to include the training, signing of a paper and actual creation of the account. NIST 800-18 4.3
- Termination procedures - the process for deleting user accounts upon termination either friendly or unfriendly needs to be completed. NIST 800-18 4.3
- Contingency Planning – it is stated in the document that a contingency plan has been created. Though the Contingency plan was not attached. This is a key document in the SSP and should be included. NIST 800-18 5.GSS.4
- Backup plan – all systems should have a backup plan. The backup plan should be attached to the SSP to include media used, storage, backup strategy and recovery. NIST 800-18 5.GSS.7

Level – Medium should be done in the near future

- System Environment section needs a topology diagram NIST 800-18 3.5
- Risk Assessment needs to be performed and documented NIST 800-18 4.1
- Value of the system needs to be determined and documented NIST 800-18 4.1
- Threat to the system need to be identified and documented NIST 800-18 4.1
- Vulnerabilities need to noted and documented NIST 800-18 4.1
- Planning for Security in the Life Cycle needs information on how media is moved, destroyed etc. NIST 800-18 4.4
- Authorized Processing – The C&A process needs to be implemented to obtain authorized processing NIST 800-18 4.5
- Production Input \ Output Controls need to be implemented and documented NIST 800-18 5.GSS.3
- Security Awareness and Training – a training program should be designed and implemented NIST 800-18 5.GSS.8

Level – Low should be done as time permits

- Least Privilege – should be implemented for users and documented NIST 800-18 5.GSS.1
- Separation of duties – should be implemented for users and documented NIST 800-18 5.GSS.1

Appendix A: Glossary

Acceptable Risk is a concern that is acceptable to responsible management, due to the cost and magnitude of implementing countermeasures.

Accreditation is synonymous with the term **authorize processing**. Accreditation is the authorization and approval granted to a major application or general support system to process in an operational environment. It is made on the basis of a certification by designated technical personnel that the system meets pre-specified technical requirements for achieving adequate system security. See also ***Authorize Processing, Certification*** and ***Designated Approving Authority.***

Authorize Processing occurs when management authorizes a system based on an assessment of management, operational and technical controls. By authorizing processing in a system the management official accepts the risk associated with it. See also ***Accreditation, Certification,*** and ***Designated Approving Authority.***

Availability Protection requires backup of system and information, contingency plans, disaster recovery plans, and redundancy. Examples of systems and information requiring availability protection are time-share systems, mission-critical applications, time and attendance, financial, procurement, or life-critical.

Awareness, Training and Education includes (1) awareness programs set the stage for training by changing organizational attitudes toward realization of the importance of security and the adverse consequences of its failure; (2) the purpose of training is to teach people the skills that will enable them to perform their jobs more effectively; and (3) education is more in-depth than training and is targeted for security professionals and those whose jobs require expertise in automated information security.

Certification is synonymous with the term **authorize processing**. Certification is the technical evaluation that establishes the extent to which a computer system, application, or network design and implementation meets a pre-specified set of security requirements. See also (***Accreditation)*** and (***Authorize Processing.***)

Confidentiality Protection requires access controls such as user ID/passwords, terminal identifiers, restrictions on actions like read, write, delete, etc. Examples of confidentiality-protected information are personnel, financial, proprietary, trade secrets, internal agency, investigations, other federal agency, national resources, national security, and high or new technology under Executive Order or Act of Congress.

Designated Approving Authority (DAA) is the senior management official who has the authority to authorize processing (accredit) an automated information (major application) or (general support system) and accept the risk associated with the system.

General Support System is 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/or

applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.

Individual Accountability requires individual users to be held accountable for their actions after being notified of the rules of behavior in the use of the system and the penalties associated with the violation of those rules.

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.

Networks include communication capability that allows one user or system to connect to another user or system and can be part of a system or a separate system. Examples of networks include local area network or wide area networks, including public networks such as the Internet.

Operational Controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Risk is the possibility of harm or loss to any software, information, hardware, administrative, physical, communications, or personnel resource within an automated information system or activity.

Risk Management is the ongoing process of assessing the risk to automated information resources and information, as part of a risk-based approach used to determine adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate cost-effective controls to achieve and maintain an acceptable level of risk.

Rules of Behavior is the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of federal government equipment, the assignment and limitation of system privileges, and individual accountability.

Sensitive Information refers to information that requires protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the information. The term includes information whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary information, records about individuals requiring protection under the Privacy Act, and information not releasable under the Freedom of Information Act.

Sensitivity in an information technology environment consists of the system, data, and applications that must be examined individually and in total. All systems and applications require some level of protection for confidentiality, integrity, and availability that is determined by an evaluation of the sensitivity and criticality of the information processed, the relationship of the system to the organizations mission, and the economic value of the system components.

System is a generic term used for briefness to mean either a major application or a general support system.

System Operational Status is either (a) Operational - system is currently in operation, (b) Under Development - system is currently under design, development, or implementation, or (c) Undergoing a Major Modification - system is currently undergoing a major conversion or transition.

Technical Controls consist of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.

Threat is an activity, deliberate or unintentional, with the potential for causing harm to an automated information system or activity.

Vulnerability is a flaw or weakness that may allow harm to occur to an automated information system or activity.

Appendix B: References

OMB Circular A-130, Appendix III

Computer Security Act, 1987

GISRA Government Information Security Reform Act

FISMA Federal Information Security Management Act

NIST 800-18 Guide for Developing Security Plans for Information Technology Systems

Appendix C: Sample System Security Plan

SECURITY PLAN

FOR

Agency NUMA Network

Certified by: _____ Date: _____
System/Application Owner

Approved by: _____ Date: _____
CIO or Designee

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

GENERAL PLAN CONTENT

This security plan contains detailed technical information about the system, its security requirements, and the controls implemented to provide protection against its risks and vulnerabilities. This security plan, at a minimum, is marked, handled, and controlled as a sensitive document. In addition, the security plan is dated for ease of tracking modifications and approvals.

I. SYSTEM IDENTIFICATION

This section of the plan provides basic identifying information about the system. Consideration was given to potential users of the plan, e.g., senior managers responsible for approving system operations, internal and external auditors, owners of interfacing systems, and owners of supporting systems.

I.A. Responsible Organization

The following organization has been designated responsibility for the system/application identified in Section I.B. below:

NUMA
123 Maple Street
Washington, DC 20001

I.B. System Name/Title

The unique identifier of NUMA Agency Network has been assigned to the system discussed throughout this security plan.

System Boundaries

NUMA Agency Network is comprised of all processing, communications, storage, and related resources located at main Headquarters. The system is comprised of desktop workstations, file and print servers, printers, modems, and routers located on the 4th and 5th floors of the NUMA HQ building.

The logical boundary for this system is behind the Cisco PIX firewall and 2900 router named NUMA III. It is connected by T1's to offsite locations of the NUMA agency around the world. In addition it is connected to the Internet via a DMZ consisting of a PIX firewall, NIDs, VPN Server and NAT server.

Multiple Similar Systems

The general support system, NUMA I, provides distributed application and telecommunications support for the remote site located in multiple locations around the worlds oceans. A "master plan" was developed for the NUMA by the organization that has the responsibility for system development, operation, and maintenance. The contents of this remote site security plan is a shorter "system site plan" that references the security plan for the NUMA (using its unique identifier) and contains information unique to the site (e.g., physical, environmental, responsible individuals, hardware, contingency plan, risk assessment, certification and accreditation/approvals

and milestone or completion dates for planned controls). System plans that reference the master plan are also listed in the master plan by their unique identifiers.

I.C. System Category

Federal guidance for security plans (OMB Bulletin No. A-130, Appendix III) establishes two system categories: Major Application and General Support System. The NUMA Agency Network system meets the criteria for a GENERAL SUPPORT SYSTEM. The system has defined functions and readily identifiable security needs.

I.D. System Operational Status

The NUMA Agency Network is in the operational phase of its life cycle.

I.E. General Description/Purpose

The NUMA Agency Network purpose is to provide connectivity and security to NUMA users for the purpose of access to internal major applications as well as connectivity to the Internet for scientific research.

The highest level of information accessed and processed on the system is "Sensitive But Unclassified" (SBU). Additional handling procedures are required for SBU processing. No classified information is permitted on the system.

I.F. System Environment and Special Considerations

The system is physically housed on the 4th and 5th floor in NUMA HQ building.

The computer room floors are enclosed with windows rated as Tempest to reduce emissions. They have floor to ceiling walls with fire suppression equipment installed. They have UPS's with generators in case of power loss.

All access to the NUMA HQ building is by guarded entrances. The employees must show badges at the door. The elevator to the 4th and 5th floors is also keyed to the badge, so personnel must have their badge programmed to take the elevator to these floors. It is also necessary to pass a retinal scan to access the computer rooms themselves.

Access to computing resources requires that the user complete the following:

- Background check
- Security training (Physical and INFOSEC)
- Management authorization

I.G. System Interconnection/Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. The sub-network NUMA Agency Network at NUMA HQ relies on the primary network NUMA I for access to the Internet and Major Applications.

The NUMA Agency Network system is directly connected to any external networks.

Connections are made via T1's with 128K blowfish encryption via VPN's

The following is specific information associated with the interconnected systems.

System Name	System Identifier	Owning Organization	Type of Connection (protocol)	Sensitivity level of the System
Agency NUMA Network	NUMA	NUMA	TPC/IP	SBU
Internet	N/A	N/A	TCP/IP	Unclassified

I.H. Information Contact(s)

The following individuals are provided as information contacts:

Title	Name	Organization	Telephone
ISSO	Michael Kirby	NUMA	123-456-7890
Security Manager	Clive Cussler	NUMA	456-789-0123
Program Manager (System Owner)	Dirk Pitt	NUMA	789-012-3456

II. SENSITIVITY OF INFORMATION

This section provides a description of the types of information handled by the system and/or the criticality of the information to accomplishing the organization's mission.
The nature of the information sensitivity and criticality are described in this section. The description contains information on applicable laws and regulations affecting the system and a general description of sensitivity as discussed below.

II.A. Applicable Laws or Regulations Affecting the System

The following apply to the Agency NUMA Network:

- OMB Circular A-130, A-123, A-127
- Freedom of Information Act of 1986 (P.L. 99-570)
- FIPS PUB 31, 41, 65, 73, 112, 113
- Computer Security Act of 1987, 40 U.S.C. 759.
- Privacy Act of 1974, 5 U.S.C. 552a (e)(10).
- Federal Manager's Financial Integrity Act, 31 U.S.C. 1352.

- Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030.
- Executive Order 10421 entitled, "Providing for the Physical Security of Facilities Important to the National Defense."
- "National Policy for Safeguarding and Control of Communications Security (COMSEC) Material," NCSC-1.
- "National Policy on Secure Voice Communications," NCSC-8.
- National Telecommunications and Information System Security Policy 3 (NTISSP 3), "National Policy for Granting Access to U.S. Classified Cryptographic Information."
- National Telecommunications and Information System Security Policy 200 (NTISSP 200), "National Policy on Controlled Access Protection."
- National Telecommunications and Information System Security Policy 300 (NTISSP 300), "National Policy on Control of Compromising Emanations."
- National Telecommunications and Information System Security Directive 500 (NTISSD 500), "National Directive on Telecommunications and Automated Information Systems Security (TAISS) Education, Training, and Awareness."
- National Telecommunications and Information System Security Directive 600 (NTISSD 600), "National Directive on Communications Security (COMSEC) Monitoring."
- "National Policy on Telecommunications and Automated Information Systems Security."
- Office of Management and Budget Circular A-123 (OMB A-123).
- Federal Personnel Manual
- The National Security Telecommunications and Information Systems Security Committee (NSTISSC) instructions and advisory memoranda.

II.B. General Description of Sensitivity

The NUMA Agency Network information must be safeguarded and protected against unauthorized use in accordance with the Privacy Act and Freedom of Information Act Programs. As such, the NUMA Agency Network is categorized as a sensitive but unclassified system in accordance with criteria established by the Computer Security Act of 1987. The information requires safeguards to ensure its confidentiality, integrity, and availability. The risk and magnitude of harm from the loss, misuse, or unauthorized access to or modification of information in the system could impact the mission and reputation of the agency. Costs associated with the losses could result in budgetary cuts and agency program reductions.

Relative Importance of Protection Needs			
	HIGH (Critical Concern)	MEDIUM (Important Concern)	LOW (Minimum Concern)
Confidentiality		X	
Integrity	X		
Availability	X		

III. SYSTEM SECURITY MEASURES

This section describes the control measures (**in place** or **planned**) that are intended to meet the protection requirements of the general support system. The types of control measures are consistent with the need for protection of the general support system described in the previous section.

III.A. Risk Assessment and Management

OMB Circular A-130, Appendix III, re-issued in 1996, no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. Risk assessment and risk management are crucial elements of the security planning process.

Describe the Risk Assessment Approach

A risk assessment HAS NOT been conducted for the NUMA Agency Network

The C&A Team plans to conduct a formal risk assessment. The risk analysis program is based on a standardized methodology that has been developed through the collective experiences and expertise of security consultants and analysts that have actually performed a multitude of risk analyses. The risk assessment approach will be the Riskman process.

Other System Evaluation Approaches

The Security staff to identify possible areas of concern conducts yearly internal system reviews. The reviews are documented and the findings are forwarded to the appropriate personnel for action. Follow-up reviews are conducted to verify actions taken.

III.B. Review of Security Controls

The NUMA agency has developed an ongoing Certification and Accreditation program by which systems and applications will be assessed for security compliance and vulnerabilities.

Describe the Type of Independent Security Review and Its Findings

An independent Certification review WILL BE conducted independent contractors on December of 2005.

The Office of the Inspector General (OIG) conducted an independent security review on November 12th 2003.

See attached appendix

III.C. Applicable Guidance

- OMB Circular A-130, A-123, A-127
- Freedom of Information Act of 1986 (P.L. 99-570)
- FIPS PUB 31, 41, 65, 73, 112, 113
- Computer Security Act of 1987, 40 U.S.C. 759.
- Privacy Act of 1974, 5 U.S.C. 552a (e)(10).
- The Immigration and Nationality Act, 8 U.S.C. 1202, Section 222(f).
- Federal Manager's Financial Integrity Act, 31 U.S.C. 1352.
- Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030.
- "National Policy for Safeguarding and Control of Communications Security (COMSEC) Material," NCSC-1.
- "National Policy on Secure Voice Communications," NCSC-8.
- National Telecommunications and Information System Security Policy 3 (NTISSP 3), "National Policy for Granting Access to U.S. Classified Cryptographic Information."
- National Telecommunications and Information System Security Policy 200 (NTISSP 200), "National Policy on Controlled Access Protection."
- National Telecommunications and Information System Security Policy 300 (NTISSP 300), "National Policy on Control of Compromising Emanations."
- National Telecommunications and Information System Security Directive 500 (NTISSD 500), "National Directive on Telecommunications and Automated Information Systems Security (TAISS) Education, Training, and Awareness."
- National Telecommunications and Information System Security Directive 600 (NTISSD 600), "National Directive on Communications Security (COMSEC) Monitoring."
- "National Policy on Telecommunications and Automated Information Systems Security."
- Office of Management and Budget Circular A-123 (OMB A-123).
- Federal Personnel Manual.
- The National Security Telecommunications and Information Systems Security Committee (NSTISSC) instructions and advisory memoranda.

III.D. Rules

The "Rules of Behavior" associated with the subject system are defined in APPENDIX C, Rules of Behavior

III.E. Security Control Measures

The following section contains a description of the security measures that protect system confidentiality, integrity, and availability.

Security Control Measure Status

For each control measure identified below specify whether the control is "In-Place**," "**Planned**," "**In-Place and Planned**," or "**Not Applicable**."**

III.E.1. MANAGEMENT CONTROLS

III.E.1.a. Assignment of Security Responsibility

The following person has assigned responsibility in writing for the security of the subject system:

Michael Kirby
123-456-7890
email@email.com

III.E.1.b. Personnel Security

In-Place: All data processing positions have been evaluated for sensitivity level. It was determined by Security that all positions require a background investigation equivalent to the SBU level prior to accessing the NUMA agencies network and sub-networks.

Access to the NUMA agencies network and sub-networks prior to receiving the appropriate background investigation requires management justification and CIO approval.

III.E.2. DEVELOPMENT / IMPLEMENTATION CONTROLS

The following development/implementation controls are to assure that adequate protection is built into the system/application during development and to ensure continued operation at an acceptable level of risk during the installation, implementation, maintenance, and operation stages.

III.E.2.a. Authorize Processing

Planned: The NUMA Agency Network at NUMA HQ will be approved for processing by the Designated Approval Authority. The date for the approval is December of 2005.

III.E.2.b. Security Specifications

In-Place: **During the design, installation, configuration, and implementation of the Agency NUMA Network, all security requirements identified in Section III.C. - Applicable Guidance, were taken into consideration.**

III.E.2.c. Acquisition Specifications

In-Place and Planned: **Appropriate technical, administrative, physical, and personnel security requirements were included in specifications for the acquisition or operation of information technology installations, equipment, software, and related services.**

IT products are evaluated prior to request for procurement. During the evaluation, the technologies are tested for vulnerabilities and reviewed for compliance with security requirements.

III.E.2.d. Design Review and Testing

In-Place: **A design review and testing was conducted on the Agency NUMA Network. The review and test consisted of a compliance verification of the system configuration with established guidelines identified in the appropriate Security Compliance Checklist.**

III.E.3. OPERATIONAL CONTROLS

Operational controls are the day-to-day procedures and mechanisms used to protect production systems/applications (or planned systems/applications when they become operational). Operational controls affect the application and system environments.

III.E.3.a. Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

a. The NUMA Agency has established personnel security procedures to ensure that all personnel-accessing Department automated information system (AIS) processing resources have:
   (1) The required access levels and need-to-know;
   (2) Appropriate supervision; and
   (3) Knowledge of their AIS security responsibilities.

Background Investigations and Personnel Selection:

a. Only individuals who meet the requirements for sensitive positions outlined in the NUMA policy may be members of the systems staff or users with special access privileges, such as operator privileges.

The data center manager and the information systems security officer (ISSO), for non-mainframe AIS, ensure that a limited background investigation (LBI) is performed for all un-cleared vendor maintenance personnel.

III.E.3.b. Physical and Environmental Protection

The following physical and environmental protections are:

In-Place: Hired guard staff, perimeter walls, badge system, retina scans and video cameras are in place to allow only authorized personnel.

III.E.3.c. Production, Input/Output

In-Place: Procedures are in place to control access to printed and electronic information. Property passes are used to control the transportation of hardware and software to and from the facility. The passes are used as audit logs.

Security has developed procedures to address the following:

- Internal/external labeling for appropriate sensitivity
- Audit trails for inventory management
- Sanitization of electronic media for reuse
- Shredding or other destructive measures for hardcopy information

III.E.3.d. Contingency Planning

In-Place: A Contingency Plan was completed for the NUMA Agency Network on November 12, 2003.

The Contingency plan is reviewed annually, or as major modifications are implemented.

III.E.3.e. Audit and Variance Detection

In-Place and Planned: Security performs independent audits on NUMA information systems and applications. The most recent was conducted on November 12th, 2003 and addressed the NUMA compliance with federal computer security requirements.

Security has developed a Certification program that will include system and application audit and variance detection.

III.E.3.f. Application Software Maintenance Controls

In-Place: In-house developed application software operating on NUMA Agency Network follow an established software development life cycle procedure during the development and operational stages. During these stages, all changes are documented, testing is accomplished using made-up data versus "live" data, and the test results are documented.

In-Place and Planned: Other application software is a copyrighted, commercial off-the-shelf product, procured by the Government. Licensing and distribution of the software is controlled by the ITCCB. ITCCB has also developed a Configuration Management program that will include reviewing, testing, and documenting modifications made to application software.

III.E.3.g. Hardware and System Software Maintenance Controls

The following hardware and system software maintenance controls are used to monitor the installation and updates to hardware, operating system software, and other system software to ensure that the hardware and software functions as expected and that a historical record is maintained of system changes. These controls are used to ensure that only authorized software is allowed on the system.

Routine Maintenance and Repair Service

All personnel who service and maintain the computer and its support systems are cleared to the level of the most sensitive material associated with the system or monitored by authorized and well qualified escorts.

The organization has established an effective preventive maintenance program to eliminate or reduce most of the need for unscheduled corrective maintenance. This program also addresses remote and off-site maintenance services.

The organization has developed an effective training program to ensure that staff members, maintenance personnel and contractors are informed of IT security and Privacy Act requirements.

Configuration Management/Change Control

Planned: ITCCB has developed a Configuration Management program that will include version control, testing, impact analysis, change identification and documentation of modifications made to systems and applications.

III.E.3.h. Documentation

In-Place: **The following is a list of documentation for the Agency NUMA Network:**

- Vendor-supplied documentation of hardware
- Vendor-supplied documentation of software
- General support system security plan
- Testing procedures and results
- Standard operating procedures
- Emergency procedures
- Contingency plans
- Disaster recovery plans
- User rules of behavior
- User manuals
- Risk assessment
- Backup procedures
- Authorize processing documents and statements

III.E.4. SECURITY AWARENESS AND TRAINING

The Computer Security Act requires Federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practice of 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.

III.E.4.a. Security Awareness and Training Measures

New hires are provided new employee orientation training prior to authorization to access Agency information. All employees and contractors involved with the management, use, design, development, maintenance or operations of the system/application are made aware of their security responsibilities and trained in how to fulfill them.

Security establishes inspection programs and maintains active training and orientation programs for employees requiring access to classified information to impress upon each employee individual responsibility for exercising vigilance and care in complying with the provisions of these regulations. These programs include a continuing review of the implementation of these regulations to insure that national security information is properly safeguarded.

III.E.5. TECHNICAL CONTROLS

This section identifies the technical controls (hardware and software) used to provide automated protection from unauthorized access or misuse, to facilitate detection of security violations, and support security requirements for systems, applications and data. Normally these types of controls are coordinated with the network and/or general support system managers.

III.E.5.a. User Identification and Authentication

The system requires user identifiers (IDs) and passwords for identification and authentication. User IDs are formulated based on the user's last and first name. (The last name with the first and second initial of the first name together up to a maximum of 8 characters.) The follow is a list of the requirements associated with passwords:

(1) Password length: The password must be a minimum of eight characters in length. If the system, which the user is accessing does not accommodate eight characters, then the user should use the maximum number of character spaces available.
(2) Password composition: The password must be composed of characters from at least three of the following four groups from the standard keyboard:
- (a) Upper case letters (A-Z);
- (b) Lower case letters (a-z);
- (c) Arabic numerals (0 through 9); and
- (d) Non-alphanumeric characters (punctuation symbols);

(3) Thereafter, users should construct their own passwords when required: at least once every six months, and when it is suspected that the password has been compromised. The latter must also be reported to the ISSO.

IDs and passwords are used not only for access control, but also user accountability. Actions associated with each account (ID and password) are logged in an audit file that can be used to trace system events to user accounts. Therefore each account is assigned to a single individual. (Sharing accounts is not permitted)

Passwords are masked (hidden from view) on the input screen when a user is logging into the system. The passwords are verified against the above required system settings prior to granting access. In addition, passwords are stored by the Network Operating System in an encrypted file, located in a restricted system directory.

After three unsuccessful login attempts, the user account is disabled. The user must contact the system administrator, in person to have the account enabled. The system administrator must verify the identity of the user prior to enabling the account.

All system default accounts are either changed or removed from the system prior to operation. In addition when the system undergoes a modification, the system administrator verifies that the default accounts are configured correctly.

III.E.5.b. Authorization/Access Controls

The network operating system access control mechanism limits who can logon, what resources will be available, what each user can do with these resources, when and from where access is available. Management, LAN, security, and key user personnel cooperate closely to implement access controls. The Network Operating System security procedures, User Security, Network File Access, Console Security, and Network Security, are highlighted below to illustrate the range of security that the sub-network provides.

Logical Access Controls

User Security. User access controls determine how, when, and where LAN users will gain access to the system. Setting up user security profiles includes the following tasks:

- Specify group security settings
- Specify settings for specific users
- Manage password security - length, expiration, etc.
- Prevent user changes to settings
- Specify logon settings
- Specify logon times
- Specify logout settings
- Specify, modify, and delete logon locations (workstation, server, and link)
- Delete a user's security
- Specify user dial-in access lists for servers

Network File Access. File security is determined by the level of security that is imposed on the directory in which the file resides. (Individual files can be secured by employing "password protection" or other security mechanisms allowed by the specific application software.). There are four levels of access:

- **Control** - the user can assign access rights on directories and subdirectories; create, modify, read, and delete files and subdirectories.
- **Modify** - the user can create, modify, read, and delete files and subdirectories.
- **Read** - the user can read and copy (and execute) any file within a directory.
- **Null** - prevents user access to a particular directory. This access right is for protecting sensitive information. (Any user not included in a directory's access rights list, directly by name or indirectly by group or list membership, has null access - which can be changed by system administrators, i.e., control access.)

Console Security. The console security/selection function allows the system administrator to prevent unauthorized persons from using the operator console. This function allows the system administrator to assign a console password, lock and unlock the console, and change the console type (i.e., assign operator functions to a workstation).

Network Security. These controls determine how outside users and servers can access the resources in the LAN over dial-up lines or intermediate networks or wide area networks. Network security tasks include:

- Specifying user dial-up access
- Specifying inter-network access

REMOTE USERS

Dial-In Access / Wide Area Networks

In-Place: Dial-in access to the NUMA Agency Network is implemented under the following conditions:

- Use of these systems is authorized for domestic use only. The user must possess a Secret (minimum) clearance and be a NUMA Direct-Hire or contract employee.
- Dial-in access is authorized only for general system user access to electronic mail and file sharing. Remote system administration and sensitive application access are not authorized.
- Remote access to the NUMA networks will be with USG computers only. Personally owned computers are not authorized for accessing NUMA networks.
- Passwords and PIN must be protected from unauthorized disclosure and must never be written down and stored with the computer hardware.
- Passwords must be changed and equipment checked by security every six months.
- The highest level of information that can be processed, stored, or transmitted is SBU. Information at the classified levels is explicitly not authorized. In the event that classified is found, the hard drive must immediately be removed. Drives found to contain classified information will be labeled, handled, and disposed of as classified material.
- SBU systems are authorized only for connection to the NUMA Internet.
- Only the network office is authorized to add, remove, or modify software and hardware configurations.
- All electronic media introduced to the remote device must be scanned by the user for viruses and other malicious code.
- Magnetic media used to store SBU files must be labeled as SBU and must remain in the physical possession of the user until such time as the media can be properly stored at a USG facility. The only exception is that at personal residences the SBU media may be locked in a container or room that only the authorized user has access.
- User and Bureau/Office System Administrators are required to report immediately to Security any loss or suspected tampering of the remote machines or peripheral devices.
- Dial-in will be to the IRM provided telephone number only.

The NUMA Agency Network, dial-in functionality, implements encryption. Only those users who complete a remote access form and are authorized are provided the necessary software and connection information required for remote dial-in.

Screen Warning Banners

The NUMA Agency Network implements screen warning banners at the client level. Each node connected, is configured to display a system warning banner identifying the following guidance and notice:

This computer is a NUMA computer system. It should be used for official U.S. Government work only. Use by unauthorized persons, or for personal business, is prohibited and constitutes a violation of 16 U.S.C. 1030 and other Federal laws. You have NO REASONABLE EXPECTATION OF PRIVACY while using this computer. All data contained herein may be monitored, intercepted, recorded, read, copied, or captured in any manner by authorized personnel. System personnel or supervisors may give law enforcement officials any potential evidence of crime, fraud, or employee misconduct found on this and all connected computer systems. Furthermore, law enforcement officials may be authorized to access and collect evidence from this system. USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES EXPRESS CONSENT TO THIS MONITORING. IF YOU DO NOT CONSENT, PLEASE PRESS ESCAPE AND SHUTDOWN THIS COMPUTER NOW. PRESS OK TO AGREE TO ALL THE CONDITIONS STATED ABOVE.

Removal of the above message from the screen requires that the user take specific action in acknowledging the warning by hitting any key to continue.

III.E.5.c. Public Access Controls (Major Applications only)

N\A

III.E.5.d. Data Integrity/Validation Controls

In-Place: **The NUMA Agency Network has been certified for processing prior to operations via the completion of a system compliance configuration checklist. The checklist verifies that the configuration associated with the operating system software and hardware requirements are in compliance with established guidelines.**

The following are some additional controls:

Malicious Programs

Controls associated with the installation of software are included in the Configuration Management program.

Virus Protection

Virus detection/elimination software is installed on all servers and workstations connected to the Agency NUMA Network. The licensing is maintained and updated by NUMA.

Operations Systems personnel automatically update software.

Message Authentication,

The NUMA Agency Network implements a Message Authentication to ensure that the sender of a message is known and that the message has not been altered during transmission.

Integrity Verification
The NUMA Agency Network only implements Integrity Verification by relying on techniques identified above.

Reconciliation

The NUMA Agency Network does not use any form of Reconciliation.

Digital Signature

Digital signatures provide an extremely high level of integrity assurance. Digital signatures provide assurance of the identity of the originator, that the originator cannot falsely deny having signed the file (non repudiation), that the file has not been modified after being signed, and that the originator intends to be bound by the contents of the file. Digital signatures are designed to meet the standards of proof required by law. Digital signatures are required to replace a hand-written signature on a commitment document (e.g., contract, funds transfer document) or if the results of a risk analysis shows that level of protection is necessary and cost-effective.

The NUMA Agency Network implements Digital Signature.

III.E.5.e. Audit Trail Mechanisms

In-Place: An audit log is maintained on the NUMA Agency Network to effectively trace actions affecting the security of the system to the responsible individual. The log is protected from unauthorized modification, destruction, and access by the limited rights assigned by the system administrator using the operating system software. The audit logs are reviewed daily by the system administrator for instances of possible abuse.

The audit log records or has the capability to record the following events:

- Use of identification and authentication mechanisms

- Introduction of objects into a user's address space (e.g., file open, program initiation, etc.)
- Deletion of objects
- Actions taken by computer operators and system administrators and/or system security officers, and other security relevant events.

For each recorded event, the audit record identifies:

- Date and time of the event
- User ID
- Origin of the event (e.g., terminal ID, MAC address, etc.)
- Type of event
- Success or failure of the event

III.E.5.f. Confidentiality Controls

In-Place: The confidentiality of information accessed and processed on the NUMA Agency Network is protected using a variety of methods. The methods involve the use of Operational, Technical, and Administrative controls defined in previous sections of this plan. See the following sections:

III.E.3.a. and b. – Operational Controls - Physical and Environmental Protection and Production Input/Output Controls,
III.E.4.a. – Security Awareness and Training – Security Awareness and Training Measures,
III.E.5.a. and b. – Technical Controls – User Identification and Authentication and Authorization/Access Controls.

III.E.5.g. Incident Response Capability (GSS only)

Incidents are investigated and responded to by the Operations personnel. They ensure that the appropriate managerial, operations and security personnel are contacted. Security has developed an Incident Response Capability to respond to security incidents in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. The capability addresses specific personnel responsibilities, training and awareness, and information sharing arrangements with other agencies.

III.E.6. COMPLEMENTARY CONTROLS PROVIDED

By Support Systems

Other Applications

Not Applicable: All applications located on the NUMA Agency Network are general support applications (i.e., WordPerfect, Word, Excel, etc.) available for use by everyone having access to the Agency NUMA Network. Therefore, no additional controls exist for these applications.

Rules of Behavior

National Underwater Marine Agency (NUMA)
Backbone Local Area Network

The rules of behavior contained in this document are to be followed by all users of the NUMA Local Area Network (LAN). Users will be held accountable for their actions on the LAN. If an employee violates NUMA policy regarding the rules of the LAN, they may be subject to disciplinary action at the discretion of NUMA management. Actions may range from a verbal or written warning, removal of system access for a specific period of time, reassignment to other duties, or termination, depending on the severity of the violation.

Work at home.

NUMA Personnel Policy Directive 97-03, dated March 10, 1997, authorizes Division Directors to designate specific employees (e.g., critical job series, employees on maternity leave, employees with certain medical conditions) as eligible for working at home. Any work at home arrangement should:

- Be in writing;
- Identify the time period the work at home will be allowed;
- Identify what government equipment and supplies will be needed by the employee, and how that equipment and supplies will be transferred and accounted for;
- Identify if telecommuting will be needed and allowed (this issue should be discussed between the requesting organization, Information Resources Management (IRM), and the SECURITY OFFICE; see Dial-in access section below); and
- Be reviewed by NUMA personnel office prior to commencement.

Dial-in access. No dial-in access is used to access LAN servers. However, if a justifiable need occurs, the IRM Division Director may authorize dial-in access to a LAN server. It is understood that dial-in access would pose additional security risks, but may become necessary for certain job functions. If dial-in access is allowed, IRMD and the SECURITY OFFICE will regularly review telecommunications logs and NUMA phone records, and conduct spot-checks to determine if NUMA business functions are complying with controls placed on the use of dial-in lines. All dial-in calls will use one-time passwords.

Connection to the Internet - Some NUMA personnel have access to the Internet. Access to the Internet is to be closely controlled by the SECURITY OFFICE. NUMA divisions, staff managers, and technicians should know that only NUMA-authorized Internet connections will be allowed, and that all connections must conform to NUMA security and communications architecture.

Protection of copyright licenses (software) –

LAN and PC users are not to download LAN-resident software.

Audit logs will be reviewed to determine whether employees attempt to access LAN servers on which valuable, off-the-shelf software resides, but to which users have not been granted access. Audit logs will also show users' use of a "copy" command; this may indicate attempts to illegally download software. Unauthorized copying of PC-based software is also prohibited.

Unofficial use of government equipment – Users should be aware that personal use of information resources – LAN and PC – is not authorized.

Use of passwords – Users are to use passwords of a length specified by the LAN system administrators – a mix of six (6) alpha and numeric characters, they are to keep passwords confidential and are not to share passwords with anyone.

System privileges – Users are given access to the LAN based on a need to perform specific work. Users are to work within the confines of the access allowed and are not to attempt access to systems or applications to which access has not been authorized.

Individual accountability – Users will be held accountable for their actions on the LAN.
This is stressed during computer security awareness training sessions

Restoration of service – The availability of the LAN is a concern to all users. All users are responsible for ensuring the restoration of services in the event the LAN is not operational.

I acknowledge receipt of, understand my responsibilities, and will comply with the rules of behavior for the NUMA Backbone LAN.

_____ _____

Signature of User Date

Last Updated: July 26th, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**