Resource Ordering and Status System (ROSS)

Professional Development Services

Task 6 – Security Function Specifications

August 23, 1999

Contract: GS-35F-4863G
Delivery Order Number: GA51
Lockheed Martin Reference Number: GA510610

Table of Contents

Tables

Figures

Appendices

1. INTRODUCTION

The Resource Ordering and Status System (ROSS) is an interagency application that will link approximately 400 federal, state, municipal, and local agency wildland incident dispatch offices to share resource order and status information. ROSS will deliver an application to all tiers of the dispatch organization that automates the business processes associated with resource ordering and statusing. The ROSS system will serve as the principal means by which manpower and equipment resources will be deployed and coordinated in response to forest fires and other dangerous and potentially life threatening natural disaster situations.

The critical nature of the ROSS operational environment, and the need to protect Agency sensitive and personnel sensitive information from unauthorized access, requires that the ROSS application and underlying technical infrastructure support appropriately high assurance levels with respect to both operational availability and information integrity.

The ROSS design team has adopted a "security-in-depth" approach in which information system security is a fundamental component of the overall ROSS system design. This approach assures that ROSS security requirements are discretely defined and addressed within an appropriate layer of the ROSS technical infrastructure.

1.1 Purpose of Document

The purpose of this document is to define the ROSS application security approach within the context of a "security-in-depth" environment.

1.2 Scope of Document

This document will provide a summary of the security analysis approach employed by the ROSS design team to determine security features to be embedded with the ROSS application design.

To provide the reader the foundations by which to assess the adequacy of the ROSS security approach, this document begins with a brief introduction of several high-level security terms. This is followed by an overview of "threat based security analysis", a very useful approach for identifying appropriate Information Security (INFOSEC) mechanisms for use in a particular operational environment.

Once the reader has been introduced to the basic security approach, security mechanisms appropriate for implementation at the application level are identified. Further discussion explains to what degree the ROSS team recommends that those mechanisms be employed and integrated within the ROSS application design.

2. TECHNICAL BACKGROUND

2.1 Security Architecture Primary Functions

The security mechanisms associated with any AIS environment can be assessed with respect to the effectiveness of the primary security functions presented in Table 1.

Table 1 - Definition of the Primary Security Functions

Security Function	Definition	Definition Source
Accountability	The property that allows auditing of activities on an AIS to be traced to persons who may then be held responsible for their actions.	NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Assurance	A measure of confidence that the security features and architecture of an AIS accurately mediate and enforce the security policy.	Glossary of Computer Security Terms, NCSC-TG-004, DoDD 5200.28, Security Requirements for Automated Information Systems (AISs), March 1988, and NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Availability	A requirement intended to assure that systems work promptly and service is not denied to authorized users. Data Availability - Data that is in place, at the time, and in the form needed by the user.	An Introduction to Computer Security: The NIST Handbook, Pub 800-12, Chapter 1, and NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.	NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Integrity	Condition that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.	NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Non-repudiation	Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity. So that neither can later deny having processed the data.	NSTISSI #4009, National Information Systems Security (INFOSEC) Glossary, June 1992
Security Management	The service by means of which security administrators initialize and maintain the system's security functions and mechanisms	GCSS Security Requirements, final draft, 25 Nov 96

However, the security functions defined in Table 1 do not address the means by which each service is achieved. A discussion of security threats and corresponding defense mechanisms provides the background for defining each of these primary security functions in terms of security mechanisms, which can be implemented with the AIS application and supporting infrastructure.

2.2 Security Threat Groups

Intentional threats to ROSS information security can be organized into eight distinct groups. The groups of INFOSEC threats, defined below, are based upon the subversive objectives for which each is employed:

- **Traffic monitoring -** To analyze traffic patterns, listen to content, or to record for later decryption/analysis.
- **Traffic tampering -** To interfere with efficient communications; to mislead and confuse the enemy by selectively modifying/inserting/deleting communications content.
- **Cryptographic attacks -** To decrypt recorded data, resulting in readable message content and, possibly, useful decryption keys for future use.
- **Unauthorized access -** To obtain information and to strategically interfere with an opponent's operations using the opponents own infrastructure services.
- **Platform corruption -** To render, or to establish the ability to render, an opponent's existing resource ineffective through selective insertion/modification/ destruction of platform services. To convert an opponent's existing resources to assets which can be employed for further subversive activity;
- **Data corruption -** To interfere with and to confuse an opponent's operations by denying access to comprehensive and reliable stored data.
- **Denial of service/system panic -** To render an opponent's existing infrastructure services unavailable for their own operational use by flooding that service with erroneous requests and/or creating conditions which place a platform/service into an unstable mode.
- **Destruction/theft of archival records -** To interfere with an opponent's ability to restore system integrity and/or data integrity by corrupting/destroying electronic archives. To obtain information through the physical or electronic theft of archival records.

2.3 Mitigation of Threat

The overall process of threat mitigation is accomplished by establishing defenses against specific categories of threats. A truly secure, defense in depth, AIS environment must have an arsenal of defensive measures capable of dealing with all known threat categories, and must be capable of accommodating new variations of threats within each category.

Although the potential threats to ROSS information security are complex and numerous, any advantage that an enemy might achieve through their practice can be effectively mitigated, so long as ROSS integrated security mechanisms focus on achieving the following objectives:

- Denying unauthorized access
- Detecting unauthorized activity
- Identifying compromised components/procedures
- Restoring component/procedural integrity

2.4 INFOSEC Defensive Measures

INFOSEC defensive measures must be available to address the full array of potential threats. Defensive measures can be implemented in the system/technical architecture, via specific hardware/software components and/or programmatic controls (i.e., operational processes/procedures) to provide protection from threats to INFOSEC security.

Eight defense groups are defined, each in terms of its respective defensive objectives, which allow INFOSEC defensive measures/mechanisms to be allocated to the infrastructure and then analyzed, comprehensively, to assure that they achieve the objectives established for that group.

The INFOSEC defense groups are structured to gather functionally similar defensive measures into logical groupings that enable them to be interpreted in a manner consistent with existing OMB security guidance.

- **Partitioning/Labeling -** To simplify the deployment and maintenance of systems/data and to facilitate the system/data integrity verification process of a single AIS, while reducing the vulnerabilities to attack to which an AIS may be subjected. To reduce losses associated with the breach of an AIS's security mechanisms. To increase likelihood of intruder detection through the combined detection mechanism's of multiple AISs. To allow security management of complex AISs to be distributed over multiple specialized support teams.
- **Mandatory Access Control -** To control access to networks/platforms/services using network imposed rule-sets based upon traffic source and/or destination, requested services, and/or traffic content/markings or labeling.
- **Discretionary Access Control -** To control access to networks/platforms/ services/data based upon a user's verifiable identity and services discretely authorized for use by that user.
- **Encryption -** To prevent the unauthorized use of stored data, transmitted information streams, and system/data archives.
- **Detection of Unauthorized Activity -** To detect unauthorized use of and tampering with network/platform resources; To assess the degree of infiltration and to determine appropriate restoration measures; To determine the information compromised and to assist in assessing possible countermeasures to minimize the advantage gained.
- **Archives/Retrieval/Restoration -** To assure that lost, destroyed, and/or corrupted systems/data can be restored in a timely manner with minimal degradation in the restored system capability and minimized loss of information resources.
- **Physical Protection -** To deny unauthorized personnel opportunities to tamper with or destroy network/platform resources. To prevent unauthorized observation of user activities and/or prevent interception of (or interference with) transmitted data streams. To reduce availability of as-is network/system configurations to unauthorized personnel.
- **Programmatic Controls -** To minimize vulnerability through well-planned architectures, implemented with reliable components. To assure that personnel are provided the guidance and tools necessary to operate in a coordinated, efficient manner to safeguard and protect network, platform, and information resources. To assure that information required for verification of the system/data integrity is available to authorized operational

personnel. To assure that contingency planning is adequate, and that alternate facilities are available and capable of supporting contingency operations.

2.5 Primary Security Functions Defined in Terms of Threats and Defenses

The following table maps the seven primary security functions introduced in Table 1 (column 1) to corresponding INFOSEC defensive measures (column 2) and to relevant threats which could be used by an adversary to undermine each respective primary security function (column 3).

Table 2 - Mapping of Security Functions to INFOSEC Defensive Measures and Threats

Primary Security Functions	**INFOSEC Defensive Measures (Defense Group/Defensive Measures)**	**Relevant Threat (Threat Group/Threat)**
Accountability	3) Discretionary Access Control D) Identification/Authentication F) Authorization 5) Detection of Unauthorized Activity G) Archives/Retrieval/Restoration H) Monitoring/Logging Auditing	2) Traffic Tampering 4) Unauthorized Access
Assurance	8) Programmatic Controls M) Operational Processes/Procedures N) Configuration Management	All Groups
Availability	1) Partitioning/ Labeling B) Application Partitioning 5) Detection of Unauthorized Activity H) Monitoring/Logging/Auditing I) Integrity Verification 6) Archives/Retrieval/Restoration J) System/Data Archives 7) Availability K) Physical Protection L) Capacity Redundancy	2) Traffic Tampering 4) Unauthorized Access 5) Platform Corruption 7) Denial of Service/System Panic 8) Destruction/theft of archival records

Primary Security Functions	INFOSEC Defensive Measures (Defense Group/Defensive Measures)	Relevant Threat (Threat Group/Threat)
Confidentiality	1) Partitioning A) Data Partitioning/Object labeling C) Platform Partitioning 2) Mandatory Access Control D) Network Traffic Control Points 3) Discretionary Access Control E) Identification/Authentication F) Authorization 4) Encryption G) Encryption 5) Detection of Unauthorized Activity H) Monitoring/Logging/Auditing 7) Availability K) Physical Protection	1) Traffic Monitoring 2) Traffic Tampering 3) Cryptographic Attacks 4) Unauthorized Access 5) Platform Corruption 8) Destruction/Theft of Archival Records
Integrity	5) Detection of Unauthorized Activity I) Integrity Verification 6) Archives/Retrieval/Restoration J) System/Data Archives	2) Traffic Tampering 4) Unauthorized Access 5) Platform Corruption 6) Data Corruption 8) Destruction/Theft of Archival Records
Non-repudiation	3) Discretionary Access Control E) Identification/Authentication F) Authorization 5) Detection of Unauthorized Activity G) Archives/Retrieval/Restoration H) Monitoring/Logging/Auditing I) Integrity Verification	2) Traffic Tampering 4) Unauthorized Access 5) Platform Corruption 6) Data Corruption

Primary Security Functions	INFOSEC Defensive Measures (Defense Group/Defensive Measures)	Relevant Threat (Threat Group/Threat)
Security Management	2) Mandatory Access Control	2) Traffic Tampering
	D) Network Traffic Control Points	
	3) Discretionary Access Control	4) Unauthorized Access
	E) Identification/Authentication	
	F) Authorization	5) Platform Corruption
	5) Detection of Unauthorized Activity	
	H) Monitoring/Logging/Auditing	6) Data Corruption
	7) Availability	
	K) Physical Protection	7) Denial of Service/System Panic
	8) Programmatic Controls	
	M) Operational Processes/Procedures	
	N) Configuration Management/ Documentation	

3. ROSS APPLICATION LEVEL SECURITY REQUIREMENTS

Only a small percentage of security mechanisms are implemented entirely at the application level as indicated in Section 2.0, Technical Background. A large percentage of the security mechanisms must be implemented within the technical infrastructure (e.g., operating system, LAN, application proxy firewall, etc.) supporting the actual application components. Many of the security mechanisms listed require maintenance and operations support activities (e.g., logging, auditing, system backups) which must be supported by adequate organizational policies, procedures, and budget. Still others involve secure operating procedures properly implemented by application users and system administrators, which in turn require resources for training and monitoring to assure compliance.

ROSS has the following basic security requirements:

- ROSS must provide 24x7 operational availability
- Only authorized individuals may access information within ROSS
- Data within the ROSS must be secure from modification/tampering by unauthorized personnel

Based upon these simple requirements and the "web-enabled" nature of the ROSS application, some level of protection in all seven primary security functions (See Table 1) is required. However, the mechanisms employed and the severity with which each mechanism is employed must be tailored based upon the nature of the ROSS application and the sensitivity of the information accessed and maintained within the ROSS AIS environment.

The ROSS application and AIS environment supports resource and ordering functions which are of critical importance to the wildfire dispatchers and fire fighting personnel. The system will contain personal information regarding thousands of federal and state employees, which, under the Federal Privacy Act, the Federal government is legally responsible for providing adequate protection. The ROSS AIS environment is important and must be protected against accidental and/or malicious tampering. However, the nature of the application and the data does not warrant the use of defenses, which would only be employed in environments with classified information (i.e., information of strategic military significance). Use of overly stringent security requirements would result in an overly cumbersome design and greatly increased implementation and operating costs.

Table 3, below, documents those ROSS INFOSEC requirements recommended for implementation at the ROSS application level, as well as those INFOSEC requirements which the ROSS development team assumes will be implemented and maintained within the ROSS operational AIS technical environment.

Table 3 - Recommended ROSS INFOSEC Requirements

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
Partitioning/Labeling		
A) Data Partitioning/Object labeling		
A1 - Data/application access control based upon data file/table/component object labeling (supporting Mandatory Access Control policies)	A1.1 - All data, received /processed by the ROSS application shall be protected as "sensitive but unclassified" information	ROSS Application Level
A2 - Automatic object labeling of printed reports and electronic media output	A2.1 - Each file or data collection in ROSS shall have an identified source and an assigned sensitivity level. Reports and files generated with data from ROSS data files will be marked with a sensitivity label corresponding to the highest level associated with any file or data collection used to generate the report.	ROSS Application Level
A3 - Physically/logically separated data tables/files based upon security level and/or access groups	A3.1 - ROSS application database files/table shall be logically and/or physically segmented to the degree necessary to adequately support application level and database level discretionary access controls.	ROSS Application Level
B) Application Partitioning		
B1 - Configuration management of application, operating system and INFOSEC functionality	B1.1 - ROSS shall employ Configuration Management version/compatibility control techniques to assure life-cycle, cohesive integration of application, operating system, and required INFOSEC functional capabilities.	ROSS Application Level
B2 - Deployment and maintenance of application, operating system, and INFOSEC functional capability	B2.1 - ROSS shall employ Configuration Management compliant distribution techniques to support the integrated deployment and life-cycle maintenance of required INFOSEC functional capabilities.	ROSS Application Level
C) Platform Partitioning		
C1 - "Hardened" operating systems/platforms ♦ **Restricted/reduced O/S and communications services** ♦ **Reduced numbers of complex executables** ♦ **Restricted issuance of O/S level accounts**	C1.1 - Operating systems, GOTS, COTS, and developmental software platforms shall be accredited by the ROSS Designated Approval Authority (DAA)	**Assumption:** ROSS AIS Environment
	C1.2 - Operating System level accounts on ROSS resources shall not be issued to users, and shall be issued to system administration personnel upon stringently enforced site operational procedures.	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
level accounts **Strict discretionary access control of O/S resources (directories, files, communications ports, etc.)** **Controls on object reuse**	C1.3 - Operating system reuse security requirements shall address how objects are cleared prior to assignment for reuse and shall protect files, memory and other objects in a system from being accessed by other users after those system resources were released by a different user.	ROSS Application Level
C2 - Physical separation of applications/databases, based on: ♦ **User community** ♦ **Classification level** ♦ **Sensitivity**	C2.1 - The ROSS DAA shall assess the sufficiency of DBMS/application based access controls and shall, if necessary, make recommendations for further logical/physical separation of applications and databases.	Assumption: ROSS AIS Environment
Mandatory Access Control		
D) Network Traffic Control Points		
D) - General Requirements	D1 - All communications connections via modems shall be subjected to controls (e.g., encryption, call back, strong authentication criteria, etc.) Modems shall not be allowed to bypass accredited Network Traffic Control Points (NTCPs) mechanisms.	**Assumption:** ROSS AIS Environment
	D2 - Gateways and proxy firewalls shall be accredited by the ROSS DAA	**Assumption:** ROSS AIS Environment
D1 - Switch/router/gateway filtering ♦ Source, destination, requested service based	D1.1 - Policy for infrastructure used by ROSS AIS environment switch, router, and gateway filtering shall be "that which is not explicitly allowed, is disallowed".	**Assumption:** ROSS AIS Environment
D2 - Application Proxy firewalls **Source/destination/requested service based**	D2.1 - All remote user access to ROSS environment client/server based applications will be controlled (e.g., via application proxy, encryption, etc.)	**Assumption:** ROSS AIS Environment
Discretionary Access Control		
E) Identification/Authentication		
E) - General Requirements	E1 - The ROSS applications shall employ ROSS DAA approved techniques for identification and authentication, prior to granting access to any ROSS application/database service or ROSS resource.	ROSS Application Level
	E2 - The infrastructure used by ROSS shall provide a trusted or encrypted communication path between the system and the user for Identification and Authentication	ROSS Application Level

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
E1 - Identification ♦ **- Logical Identification** ♦ **- User_ID** ♦ **- Host Address** ♦ **- IP number** ♦ **- Physical Identification** ♦ **Smart ID cards/buttons** ♦ **Biophysical identification**	E1.1 - ROSS shall support logical identification and/or physical identification mechanisms.	ROSS Application Level
	E1.2 - ROSS shall verify available connection data (i.e., source IP address, time of connection, etc.) for consistency with authorized user profiles.	ROSS Application Level
E2 - Authentication ♦ **Passwords/complex password enforcement** **Smartcards/one-time use passwords** ♦ **Trusted-user/trusted-host** ♦ **Public Key/certificate based**	E2.1 - ROSS DAA accredited password integrity policies shall be stringently enforced in Sensitive But Unclassified (SBU), single application environments.	ROSS Application Level
	E2.2 - ROSS applications and databases, in support of single point/unitary logins to SBU application/data environments, shall support identification/authentication processes (e.g., accept token/certificates, smartcards, etc.)	ROSS Application Level
F) Authorization		
F1 - Centralized vs. Distributed/Tiered Authorization	F1.1 - Authorization of user access shall be distributed to the degree necessary to avoid authorization/processing bottlenecks and to assure approval is granted by one knowledgeable of the requesting user's need to know.	ROSS Application Level
	F1.2 - Authorizing personnel shall be held accountable for all user's granted access to ROSS services and resources based on their approval.	ROSS Application Level
F2 - Basis for Granting ♦ **Need for services/need-to-know**	F2.1 - Employment and established need-to-know criteria shall be the basis for granting users access to specific ROSS services and data.	**Assumption:** ROSS AIS Environment
	F2.2 - The identity, organization, mission need, and need-to-know of persons requesting access to ROSS services/data shall be verified by authorizing personnel prior to approval of access.	**Assumption:** ROSS AIS Environment
F3 - Scope of Authorization ♦ **Single application, multi-application** ♦ **Single database, multiple databases**	F3.1 - ROSS shall function so that each user has access to all services and information to which the user is entitled (by virtue of formal access approval), but to no more. ROSS information access must be directly essential to the accomplishment of lawful and authorized Government purposes.	ROSS Application Level
	F3.2 - The capability to dynamically assign and manage access permissions (e.g., password management) shall be provided.	ROSS Application Level

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
F4 - Granularity of Control ♦ **- Organization, group, individual** ♦ **- Network /subnet access** ♦ **- Application access** ♦ **- Database/table/data component access**	F4.1 - Each authorized ROSS user and resource shall have a unique system identity.	ROSS Application Level
	F4.2 - ROSS shall provide the ability to define and control access between named users and named objects (e.g., files, attributes, programs).	ROSS Application Level
	F4.3 - Access controls shall be specified to the granularity of the individual user.	ROSS Application Level
	F4.4 - Access controls shall be capable of supporting access to information based on user's individual identity or the role of a user at a particular time. The latter is usually referred to as Role Based Access Control (RBAC).	ROSS Application Level
Encryption		
G) Encryption		
G1 - Network control point encryption, decryption, re-encryption	G1.1 - ROSS Identification/Authentication shall be encrypted.	ROSS Application Level
	G1.2 - ROSS shall support optional encryption of transmissions between the ROSS application server and ROSS clients.	ROSS Application Level
G3 - Standardized/certified proved encryption algorithms (DES, RSA, SSL, etc.)	G3.1 - ROSS shall employ accredited encryption algorithms.	ROSS Application Level
Detection of Unauthorized Activity		
H) Monitoring/Logging/Auditing		
H1 - Network Control Point level/Network Manager Level/Platform Level	H1.1 - Traffic/event monitoring/logging and automated alert responses shall be implemented at Network Traffic Control Points, the Network Manager Level, and the application platform level, as practical, to support enforcement of the operational facility security policies.	**Assumption:** ROSS AIS Environment
	H1.2 - ROSS GOTS/COTS hardware and software for which monitoring, logging, and auditing requirements are established shall be compatible with accredited auditing tools.	**Assumption:** ROSS AIS Environment
	H1.3 - Logs and auditing tools shall support, at a minimum, auditing options by group/user/role, activity performed (e.g., database operation), object accessed, date/time of occurrence. Auditing capabilities shall include support for correlating multiple audit tables.	ROSS Application Level
	H1.4 - The established audit trail shall contain sufficient detail to reconstruct events when determining if a compromise has taken place and if so, the severity and extent of the compromise of all affected application and data resources.	ROSS Application Level

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
	H1.5 - All logs shall be protected by safeguards which detect and prevent inadvertent modification or destruction of data, and detect and prevent malicious destruction or modification of data in accordance with accredited operational facility procedures.	**Assumption:** ROSS AIS Environment
H2 - Traffic logging (source, destination, any additional information available)	H2.1 - Traffic shall be monitored and information pertaining to traffic source, destination, connection start/stop and other data capable of being used to verify users identities and physical location shall be logged in accordance with accredited operational facility procedures.	**Assumption:** ROSS AIS Environment
H3 - Event logging (user actions, user attempted actions, alarms, system status)	H3.1 - The ROSS application shall maintain system event logs capable of assuring that user actions are open to detailed review. The audit events shall include, at a minimum: login/logout, select application user/administrator actions; authorization/security violations; failed/successful file system access attempts (i.e., read, modification, and deletion events); and attempts to bypass security features. Each operational site/application may include additional events, as dictated by mission requirements.	ROSS Application Level
	H3.2 - DBMS audited events shall include: login/logout, select DBMS user/administrator actions, database files/tables/elements read, modified, and/or deleted; authorization/security violations; and attempts to bypass DBMS security features.	ROSS Application Level
H4 - Automated alerts (messaging, alarms, paging)	H4.1 - ROSS shall provide the means to set threshold conditions, which upon triggering, generate automated alerts and or implement pre-programmed or rule-based actions.	ROSS Application Level
H5 - SNMP messages/maintenance action logs ♦ **Monitoring of hardware related events (off-line, unavailable, etc)**	H5.1 - Operational facility accredited auditing procedures shall stress analysis of automatically generated platform and network hardware/software status/error messages as a means mitigating operational risks and detecting malicious intrusions.	**Assumption:** ROSS AIS Environment
	H5.2 - Accredited auditing tools shall support the integrated review of automatically generated platform and network hardware/software status/error messages with all other logged events.	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
H7 - Decoys and Ploys ♦ **Used to determine intent and level of knowledge/skill of an opponent**	H7.1 - Based on a risk versus cost analysis, operational environments shall establish, monitor, and maintain a sufficient number of decoy devices and ploys to assist operational site security managers in ascertaining the identity, level of knowledge, skill, and malicious intent of suspected intruders without placing mission oriented resources at risk. Sufficient operational facility resources shall be expended to assure that decoys and ploys are convincing, enticing, and effective in achieving their intended purpose.	**Assumption:** ROSS AIS Environment
I) Integrity Verification		
I1 - Static file ♦ **Software accreditation/CM** ♦ **Checksums, electronic file signatures**	I1.1 - Operational facility accreditation shall require the existence of automated procedures for the verification of system integrity, which shall include the verification of all network component and platform semi-static and static files. This can be based upon verification against configuration-controlled checksums, electronic file signatures, or other mechanisms.	**Assumption:** ROSS AIS Environment
I2 - Dynamic files ♦ **DBMS rollback files** ♦ **OS/application/database activity/event log files**	I2.1 - Data which is incoming source data to a ROSS application or database shall be archived, including incoming source data records that are marked for deletion. The archive shall include: ♦ The date-time receipt; ♦ The authenticated identity of the source; ♦ Nature of any error(s) detected. This recording will support non-repudiation of the receipt of data and the ability to recreate scenarios, which may have led to the corruption of the ROSS databases.	**Assumption:** ROSS AIS Environment
	I2.2 - Security features shall be implemented upon application servers and within databases associated with ROSS, and provide log based indicators of data integrity problems. See H3 - Event Logging.	ROSS Application Level
	I2.3 - Databases associated with ROSS shall maintain database rollback logs, which can be used to correct inadvertent or malicious changes to ROSS data, once detected.	ROSS Application Level
	I2.4 - Regular system/data backups using operational facility accredited backup procedures shall be implemented to mitigate operational impacts due to loss/corruption of dynamic files.	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
I3 - Virus Detection Software	I3.1 - The ROSS environment shall incorporate virus protection software, which protects against malicious code, and is accredited for use within their respective operating environments. This shall include protection against JAVA, Active-X and similar type codes.	**Assumption:** ROSS AIS Environment
I4 - Security Probes	I4.1 - Operational facility System Administrators shall verify the security of their own internal networks through the periodic use of accredited automated security probes. The operational site DAA shall approve all procedures involving the use of automated security probes.	**Assumption:** ROSS AIS Environment
Archives/Retrieval/Restoration		
J) System/Data Archives		
J1 - Incremental/full backups ♦ **General backups** ♦ **Date based** ♦ **Targeted backups** ♦ **Platform/OS/ application/component**	J1.1 - ROSS applications and operational facilities shall support the ability to perform system and data backups, per current NITC guidance.	ROSS Application Level
	J1.2 - ROSS applications and operational facilities shall support the ability to recover from failures using system and data backups, per current NITC guidance.	ROSS Application Level
	J1.3 - ROS related audit data should be permanently maintained and archived. See Also - I2.1, I2.4	**Assumption:** ROSS AIS Environment
J2 - Integrity verification of archived components prior to archive	J2.1 - Integrity verification shall be performed of system/application/data files prior to creation of system restoration archives and shall be included in the archives configuration management catalog.	**Assumption:** ROSS AIS Environment
J3 - Encryption of archived files	J3.1 - Encryption of archival tapes in classified environments is not required.	**Assumption:** ROSS AIS Environment
J4 - Tape checksum generation[1]	J4.1 - Archive tapes procedures shall incorporate means by which the authenticity/integrity of archival tapes can be established prior to use.	**Assumption:** ROSS AIS Environment

[1] Gray areas indicate requirements associated with operational level or programmatic implementation rather than requirements oriented to applications or infrastructure.

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
J5 - Controlled cataloging/CM	J5.1 - Configuration control shall be maintained over all archived records. CM controls shall include the ability to identify: date archive was produced; operational facility/platforms(s)/system(s) archived; file name/size/other descriptors contained on the tape; and tape/file integrity verification parameters.	**Assumption:** ROSS AIS Environment
J6 - Physical protection against theft, modification, destruction	J6.1 - Off-site storage shall be accredited for the physical protection of the highest classification/sensitivity level of information contained on the archived tape.	**Assumption:** ROSS AIS Environment
J7 – Physical storage/off-site storage	J7.1 - The ROSS operational site shall provide, offsite storage of archived records.	**Assumption:** ROSS AIS Environment
Availability		
K) Physical Protection		
K1 - Certification of hardware components	K1.1 - Server platforms shall be certified by the ROSS DAA for handling Sensitive but Unclassified information.	**Assumption:** ROSS AIS Environment
K3 - Physical access control to server platforms, network components, cabling, workstations	K3.1 - Access to network infrastructure components (e.g., routers, bridges, servers, etc.) shall be controlled and limited to personnel with a demonstrated need for access.	**Assumption:** ROSS AIS Environment
L) Capacity/Redundancy		
L1 - Planned over-capacity	L1.1 - Operational facility and communications system/technical architectures shall provide the means to provide additional capacity to meet projected short term growth (1 year) and to accommodate all immediate operational facility contingency planning either with existing capacity or through pre-coordinated modular expansion capable of implementation within 6 months.	**Assumption:** ROSS AIS Environment
L2 - Modular expandability	L2.1 - ROSS GOTS/COTS/developmental hardware and software components shall comply with all applicable OMB standards for open system compliance.	ROSS Application Level
	L2.2 - System/operational facility accreditation processes shall verify that accredited OSI hardware/software components have been integrated within operational, system, and technical architectures which support modular expandability with respect to both overall system capability and expanded user capacity	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
L3 - Use of accredited/certified components	L3.1 - All platform/network components shall comply with the respective ROSS DAA accreditation/certification requirements.	**Assumption:** ROSS AIS Environment
L4 - Multiple independent primary transmission paths	L4.1 - ROSS communications services shall be assured against malicious attacks that would result in a single point of failure in the processing or delivery of mission planning, execution, and monitoring information.	**Assumption:** ROSS AIS Environment
L5 - Automated rerouting	L5.1 - The capability to detect the failure of a system or network service shall be provided.	**Assumption:** ROSS AIS Environment
	L5.2 - The capability to redirect communications to alternate processing nodes and/or across alternate transmission paths, based upon detection/analysis of system/network failures/congestion shall be provided.	**Assumption:** ROSS AIS Environment
Programmatic Controls		
M) Operational Processes/ Procedures		
M1 - Accreditation processes	M1.1 - The ROSS application or database shall be accredited by the ROSS DAA to operate in conjunction with an approved set of security safeguards. Applications shall be re-accredited at designated intervals or following major changes.	**Assumption:** ROSS AIS Environment
	M1.2 - Each operational facility shall be accredited by the ROSS DAA for local operations. The operational facility accreditation processes shall assess the sufficiency of each respective security function/procedure based upon the criticality of activities supported by the operational site and the classification/sensitivity of the data associated with those activities.	**Assumption:** ROSS AIS Environment
	M1.4 - After a security incident is known to have occurred, the seriousness of damage to ROSS data integrity and operational effectiveness shall be determined and appropriate measures taken to minimize the adverse effect	**Assumption:** ROSS AIS Environment
M2 - Application, operating system, DBMS system administrator operating procedures	M2.1 - Persons responsible for the maintenance and operation ROSS applications and databases shall be trained and tested with respect to proper operational and security-related procedures prior to any delegation of operational responsibility.	**Assumption:** ROSS AIS Environment
	M2.2 - Operational site accreditation shall incorporate testing of operational staff's proficiency with respect to proper security and recovery related procedure.	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
M3 - LAN/WAN component system administrator operating procedures	M3.1 - LAN/WAN communications support personnel shall be trained and tested with respect to proper operational and security-related procedures prior to any delegation of operational responsibility.	**Assumption:** ROSS AIS Environment
	M3.2 - Operational site accreditation shall incorporate testing of operational staff's proficiency with respect to proper security and recovery related procedure.	**Assumption:** ROSS AIS Environment
M4 - User operating instructions/operational security procedures	M4.1 -Security education, training, and awareness programs shall be enhanced to cover ROSS unique security training needs.	**Assumption:** ROSS AIS Environment
	M4.2 - The effectiveness of user training shall be monitored through the use of periodic, user community "spot checks" designed to measure the user community's retained knowledge of ROSS security policies and procedures.	**Assumption:** ROSS AIS Environment
M5 - Continuity of operations planning	M5.1 - Operational facilities shall implement a risk management program to determine how much protection is required by the AIS, the level provided, how much exists, and the most economical way of providing the needed protection.	**Assumption:** ROSS AIS Environment
	M5.2 - Operational facilities shall develop and test a contingency plans to ensure AIS security controls function reliably, and are maintained continuously during periods of interrupted service. Ensure the plan includes procedures to recover data that has been modified or destroyed.	**Assumption:** ROSS AIS Environment
N) Configuration Management/Documentation		
N1 - Operational, system, technical architectures; system requirements / design/implementation documents	N1.1 - ROSS design documentation shall provide sufficient technical detail to support smooth implementation, maintenance, and troubleshooting by operational personnel.	ROSS Application Level
	N1.2 - ROSS design documentation shall document all security features, including their proper use and maintenance, and shall provide all technical details required to integrate the application with common infrastructure security components.	ROSS Application Level

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
N2 - Local and Wide Area "As-is" logical/physical layouts	N2.1 - ROSS operational facilities shall require CM controlled logical/physical layouts of the "as-is" architecture, which include full explanatory written technical descriptions of the following: ♦ Site cable distribution plant, including network backbones, building distribution plants, and demarcation points; ♦ IP address schemes, including all current network/platform components IP assignments; ♦ Platform/network component locations and assigned physical/logical port connections to all network components; ♦ Network component routing/filtering/proxy/mandatory access control policies; and ♦ WAN connections, and level of service, and connectivity maintenance Points of Contact.	**Assumption:** ROSS AIS Environment
N3 - As-is platform software architectures	N3.1 - ROSS operational facilities shall require CM control over the "As-Is" software architectures installed on every application/database server supported. For each platform, the following shall be maintained: ♦ Logical/physical pictorial representations of the software communications stack, application interfaces, application components and database components; ♦ Data exchanges with application/database components on the same platform and local platforms; and ♦ Data exchanges with remote application/database servers and remote user populations;	**Assumption:** ROSS AIS Environment
N4 - HW/SW item configuration management	N4.1 - Operational facilities shall maintain configuration management and control over all GOTS/COTS/developmental network/application components and configurations. CM controlled components shall include names, version numbers, file sizes, and integrity checksums for the following: ♦ Application files; ♦ Configuration files; ♦ Routing tables, filter rules, proxy control; discretionary access control tables ; and ♦ Maintenance support Points of Contact;	**Assumption:** ROSS AIS Environment

INFOSEC Defense Groups, Defensive Measures/Mechanisms	Recommended ROSS Security Requirements	Recommended Layer for Implementation
N5 - Configuration management of database structures/content	N5.1 - Operational facilities shall establish configuration management over all database/table/field structures. Furthermore, CM shall be exercised over the following information: ♦ Database/table descriptions which define the purpose/user community of each database/table; ♦ Classification level(s), sensitivity level(s) associated with the database/table; ♦ Memorandums of Agreement for each separately maintained database/table which documents the originating source of the data and the organization(s) currently responsible for maintaining database/table content; ♦ Access control criteria and/or organizations responsible for authorizing access to database and/or proofs of authorization to be accepted.	**Assumption:** **ROSS AIS Environment**

4. Recommended (Preliminary) ROSS Security Architecture

Figure 5.0 presents a high-level technical architecture depicting open system based ROSS application components with COTS based security components. Details with respect to specific ROSS application components design features, and COTS security component features will be addressed to greater detail within the ROSS System Design Document and in later revisions of the ROSS Security Functional Component Document.

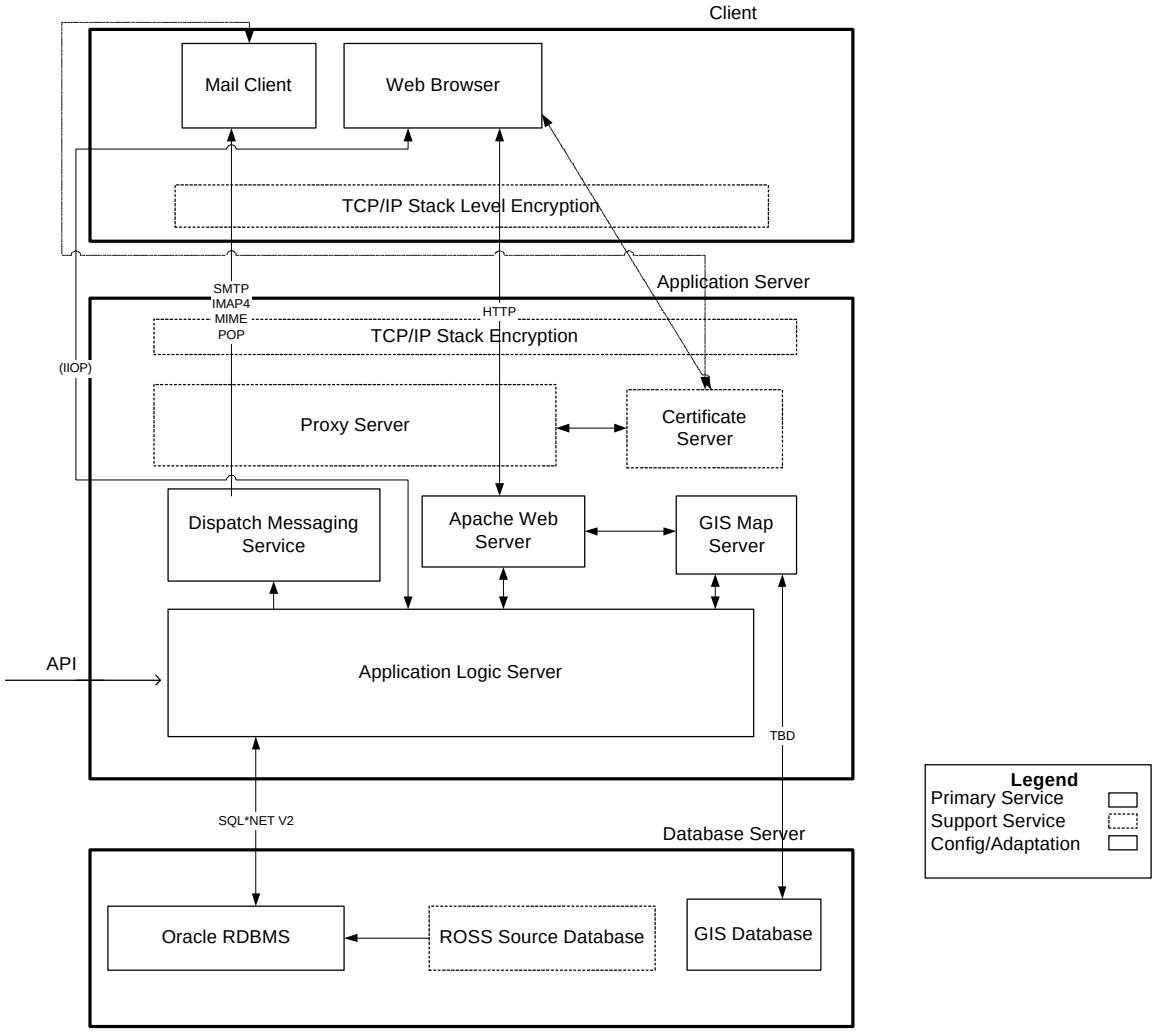

Figure 1- Preliminary ROSS Application Architecture

5. Recommended ROSS Security Roles and Responsibilities

As addressed in Sections 3.0, and 4.0, a large percentage of the recommended ROSS security mechanisms require maintenance and operation support activity (e.g., logging, auditing, system backups) which must be supported by adequate organizational policies, procedures, and budget. Still others involve secure operating procedures properly implemented by application users and system administrators, which in turn require resources for training and monitoring to assure compliance.

To assure that such activities are effectively implemented for the duration of the ROSS applications operational life, it is necessary to explicitly define roles and to explicitly assign responsibilities to those roles.

Such an effort is beyond the ROSS design team's authority. However, to facilitate the Forest Service, ROSS user community, and the ROSS deployment site operations personnel in this effort, a sample Roles and Responsibility template is provided at Appendix A. This template is currently compatible with the security requirements recommended in Sections 3.0, and the security approach presented in Section 4.0. Review of this template is recommended, and roles and responsibilities tailored to effectively match the ROSS user and operations support community.

Appendix A. Organization Configuration Chart & Roles / Responsibilities

A-1.0 OVERVIEW

A description of the ROSS security organization hierarchy is provided in Figure A-1. Five designated positions are indicated:

- Designated Approving Authority (DAA) - The ROSS DAA, ROSS Security Services, is the final authority for approving the operation of ROSS AISs;
- Component Security Manager (CSM) - The CSM is responsible for overseeing the implementation of security policy and information security programs for all ROSS AIS's and operating units;
- Office Security Manager (OSM) - The OSM is responsible for cross-unit / cross-organization security related coordination, including verification of personnel employment status
- Information Systems Security Officer (ISSO) - The ISSO is responsible for orchestrating ROSS physical and AIS security at an individual ROSS AIS facility or operating unit;
- Directorate Level Terminal Area Security Officer (TASO) - Directorate Level TASO's report directly to the ISSO and are responsible for assigned non-technical AIS security policy implementation;
- Functional Level Terminal Area Security Officer (TASO) - Functional Level TASO's report directly to the ISSO and are responsible for technical security with respect to an assigned ROSS capability or function.

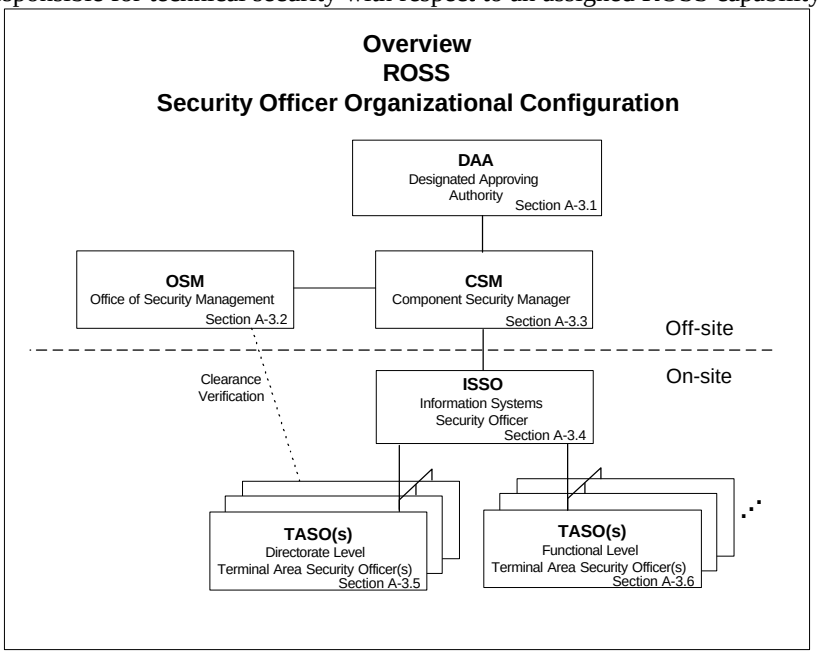

Figure A-1 - ROSS Security Organization Hierarchy

The actual number of number of TASO's required to support the CSM, OSM, and ISSO, may vary over time.

A-2.0 SPECIFIC ROSS ORGANIZATION

Figure A-2, contains a specific listing of the ROSS security officers, their specific areas of responsibility, and provides a means by which to contact them. Figure A-2, will be reviewed on a monthly basis by the CSM and ISSO to assure continued accuracy.

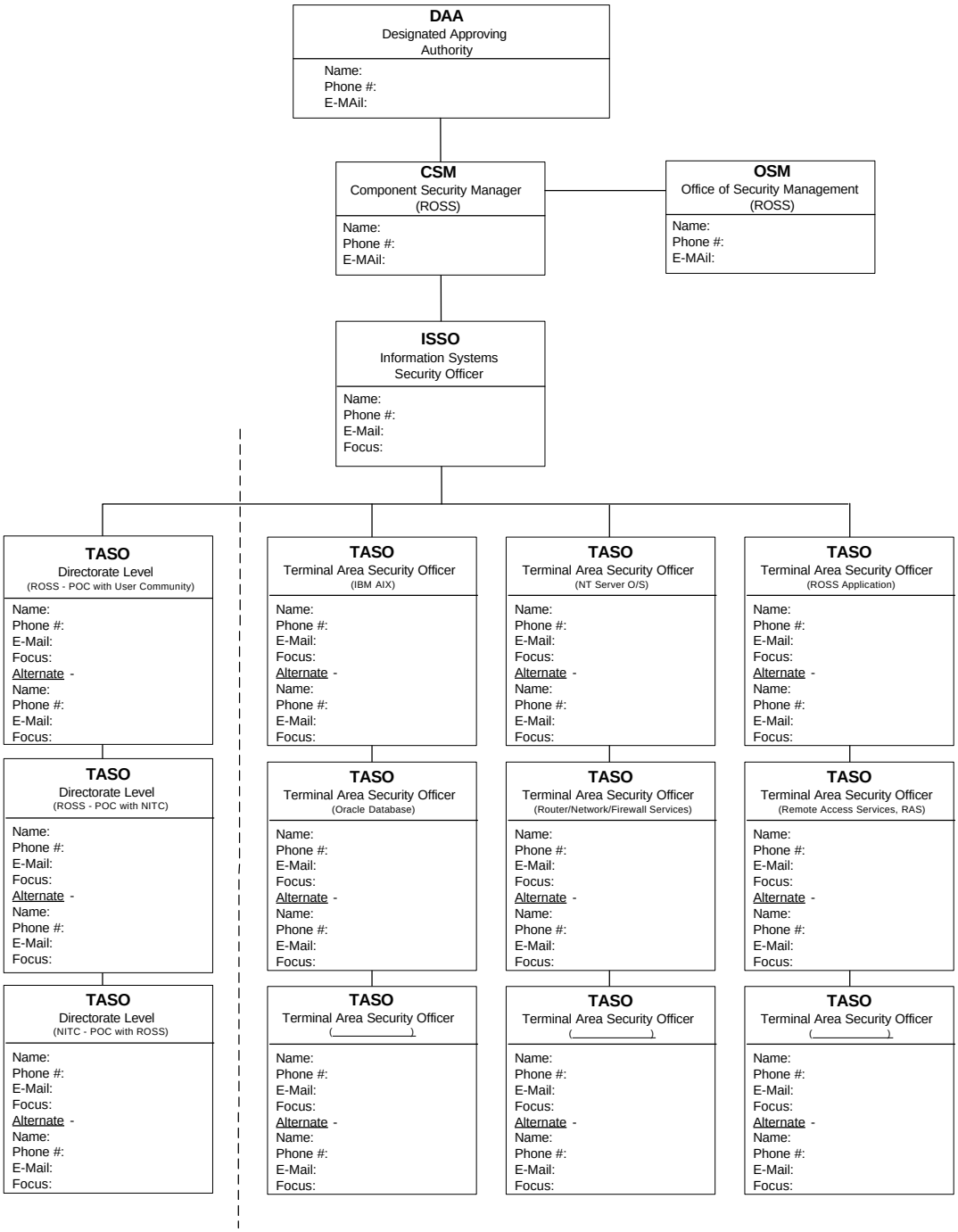

Figure A-2 - ROSS Security Organization

A-3.0 ROLES AND RESPONSIBILITIES

A-3.1 Designated Approving Authority (DAA)

The ROSS DAA, ROSS Security Services, is the final authority for approving the operation of ROSS AISs. The DAA shall:

- Provide final approval for operation of a ROSS AIS or ROSS operations facility;
- Review the ROSS Automated Information Security Plan (AISSP) and all associated accreditation documentation provided by the Component Security Manager (CSM), and confirm that the residual risk complies with AIS security requirements;
- Assist the CSM in defining system security requirements for acquisitions;
- With the CSM, provide final approval for the use of "shareware", "freeware", or "public domain", or “downloaded” SW within the ROSS operations facilities;
- With the CSM, provide final approval for the installations of all purchased/licensed software and additional copies of licensed software;

A-3.2 Component Security Manager (CSM)

The CSM is responsible for implementing security procedures and information security programs applicable to all personnel, AIS's and operations facilities. The CSM shall:

- Take appropriate action to ensure implementation of OMB policies and procedures includes AIS security education and AIS training;
- Act as the focal point for policy and guidance in ROSS security matters;
- Develop and administer AIS security programs that implement policy and regulations that are consistent with OMB guidance;
- Advise the DAA about the use of specific security mechanisms within ROSS AIS's and operations facilities;
- Provide periodic briefings to ROSS management, and to the DAA, regarding ROSS security;
- Report security vulnerabilities, maintain a record of ROSS security-related incidents (i.e., system attacks, virus incidents, etc), and report serious and unresolved violations to the DAA;
- Administer a ROSS security and training awareness program;
- Ensures that the addition of software, hardware, firmware will not degrade the security of the system;
- Retain final approval authority over:
  - all media sanitization/destruction procedures adopted; and
  - password and encryption processes adopted;
  - specific grants by the Information Systems Security Officer (ISSO) / Terminal Area Security Officers (TASO’s) of multiple user-IDs or multi-login capability to the ROSS by a single user;
- With the DAA, retain final approval authority over the installation of all purchased/licensed software and the installation of additional copies/revisions of licensed software;
- With the DAA, retain final approval authority over the use of "shareware", "freeware", "public domain", or “downloaded” SW within the ROSS facility;
- With the ISSO, review and update, on a monthly basis, the ROSS security officer organizational chart contained within Figure A-2 of this appendix;
- With the ISSO, retain responsibility for the design and implementation of an ROSS “Demilitarized Zone” (DMZ)/Firewall;
- With the Directorate Level TASO’s, ensure that all software is periodically inventoried against ROSS license agreements;
- Support the ROSS security and maintenance process (Section A-4.0);

- Support the Security Clearance/Access Control List (ACL) verification process (Section A-5.0);
- Designate to the DAA, in writing, an Office Security Manager (OSM) and an Information Systems Security Officer (ISSO);
- Have authority to delegate any and all responsibilities to the Office Security Manager (OSM) and to the ISSO, as appropriate.

A-3.3 Office Security Manager (OSM)

The OSM is responsible for personnel clearance and physical security at the ROSS AIS and operations facilities. This does not include AIS security, which is the responsibility of the ISSO, as indicated in the section below. The OSM shall:

- Lead the identification/consolidation/resolution of physical facility security issues;
- Review and provide input to the ROSS AISSP and revisions (Section A-4.0);
- Maintain and disseminate, as needed, to the CSM and ISSO/TASO's, highly accurate AIS user security clearance/status information;
- With the ISSO/TASO's, establish and retain final approval authority over local escort procedures and maintain a list of escort personnel;
- Proactively support and enforce the Security Clearance/Access Control List (ACL) verification process (See Section A-5.0).

A-3.4 Information Systems Security Officer (ISSO)

The ISSO is the on-site official responsible for implementation of ROSS AIS and operations facility security. The ISSO shall:

- Implement the responsibilities of the CSM;
- Ensure all ROSS AIS's and operations facilities are operated, used, and maintained in accordance with internal security policies and practices;
- Ensure AISs are accredited by the DAA before processing SBU information;
- Ensure that required audit trails are reviewed periodically. Also ensure that audit records are archived for future reference;
- Initiate protective or corrective measures if a security problem is discovered;
- Report security incidents in accordance with OMB Guidance, and to the CSM when security on an AIS or at a ROSS operations facility is compromised;
- Report the security status of ROSS AISs to the CSM;
- Evaluate known vulnerabilities to ascertain if additional safeguards are needed;
- Conduct periodic AIS security evaluations to ensure compliance requirements;
- With the CSM, review and update, on a quarterly basis, the ROSS security officer organizational chart contained within Figure A-2 of this appendix;
- With the CSM, retain responsibility for the design and implementation of an ROSS DMZ/Firewall;
- With the TASO's, ensure that users are aware of ROSS policies concerning unauthorized use of the AIS(s);
- With the TASO's, ensure that AIS users are not granted multiple user-IDs or multi-login capability to the ROSSe AIS, without specific exemption approved by the CSM;
- With the TASO's, ensure that the AIS(s) are used only in a manner consistent with the ROSS policies contained herein and OMB Guidance;
- Support the ROSS security and maintenance process (See Section A-4.0);

- Support the Security Clearance/Access Control List (ACL) verification process (See Section A-5.0);
- Identify to the CSM, in writing, the names of designated primary and alternate Terminal Area Security Officers (TASO's);
- Have authority to delegate specific responsibilities to TASO's, as appropriate.

A-3.5 Directorate Level Terminal Area Security Officer (TASO)

A Directorate Level TASO reports directly to the ISSO and is responsible for AIS security policy implementation with respect to an assigned ROSS directorate. A Directorate Level TASO's shall:

- Implement the non-technical AIS and personnel responsibilities of the ISSO; Accept responsibility for any ISSO responsibility so delegated;
- Ensure that all equipment processing sensitive information are properly accredited by the DAA;
- Ensure that all individuals accessing AIS's have an appropriate security clearance and need-to-know;
- Ensure that assigned personnel read and sign the AIS security awareness statement before they are authorized to use the AIS's;
- Ensure that each person using an AIS annually reads and understands the procedures for processing SBU and/or unclassified information on the AIS;
- Perform evaluations of AIS security problems in their assigned offices(s) and notify the ISSO of all security violations and any practices that may compromise system security;
- If applicable, collect and review selected remote facility audit records, document any reported problems, and forward them to the ISSO;
- Participate in automated security training and awareness;
- Not alter the configuration of an AIS as stated in this AISSP without prior approval from the ISSO and submitting an appropriate change to the AISSP;
- Ensure that the AIS is protected from theft or physical abuse and that it is used for official business only;
- Report any AIS configuration, location, layout, or procedural changes to the ISSO. This includes ensuring that the CSM inventory is accurate;
- Ensure that required waivers and approvals (e.g., for shareware, multiple user ID's, etc.) are obtained, as applicable;
- Conduct periodic AIS security evaluations to ensure compliance requirements;
- Report security incidents in accordance with OMB Guidance, and to the CSM when an AIS is compromised;
- With the OSM, establish local escort procedures and a list of escort personnel;
- With the ISSO/TASO's, ensure that users are aware of ROSS policies concerning unauthorized use of the AIS(s);
- With the ISSO/TASO's, ensure that the AIS(s) are used only in a manner consistent with the ROSS policies contained herein and OMB Guidance;
- With the ISSO/TASO's, ensure that AIS users are not granted multiple user-IDs or multi-login capability to the ROSS AIS, without specific exemption approved by the CSM;
- Ensure that preventive maintenance is performed for all AIS components as prescribed by the manufacturer or in accordance with purchase or lease warranty conditions;
- With the AIS users, ensure that all maintenance activities are observed by authorized escorts;
- Manually check media contents to determine/verify security classification, as required;
- With designated system audit managers, review logged information weekly;
- Report any suspected mishandling of an AIS or its media;
- Approve sharing of passwords, only when absolutely required;

- Ensure that automated procedures are established to assure that AIS users are restricted to a single consecutive login;
- Ensure that all users are briefed yearly concerning their AIS security responsibilities;
- With the CSM, ensure that all software is periodically inventoried against the ROSS license agreement;
- Serve as single point of contact for AIS users to obtain "shareware", "freeware", "public domain", or “downloaded” SW which has been approved by the DAA and CSM;
- Support the AISSP development and maintenance process (See Section A-4.0);
- Support the Security Clearance/Access Control List (ACL) verification process (See Section A-5.0).

A-3.6 Functional Level Terminal Area Security Officer (TASO)

Each Functional Level TASO reports directly to the ISSO and is responsible for technical security with respect to an assigned ROSS capability or function. The Functional Level TASO’s shall:

- Implement the technical responsibilities of the ISSO with respect to an assigned ROSS capability or function; Accept responsibility for any ISSO responsibility so delegated;
- Implement and maintain discretionary access control mechanisms associated with their assigned area of technical responsibility;
- Assure that backup procedures implemented for with their assigned area of technical responsibility are sufficient to restore systems to secure operational mode following system failures, as well as following intentional malicious interference;
- Assure that adequate alarms are set and that sufficient event logging is performed so that malicious interference attempts can be detected/recorded, and the severity of attacks can be assessed;
- Assure that event logs are recorded and stored in a secure manner, inaccessible to malicious tampering;
- Periodically review event logs to identify attempts to breach established security mechanisms;
- Subscribe to all relevant security and patch related services associated with their assigned area of technical responsibility; demonstrate diligence in assessing their relevance to ROSS infrastructure components;
- Maintain configuration management over assigned area of technical responsibility and assure that all relevant system/security patches are appropriately applied;
- Ensure all AISs associated with their assigned area of technical responsibility are operated, used, maintained, and disposed of in accordance with internal security policies and practices;
- Ensure AISs associated with their assigned area of technical responsibility are accredited before processing SBU information;
- Initiate protective or corrective measures if a security problem is discovered.
- Report security incidents in accordance with OMB Guidance, and to the CSM when an AIS is compromised;
- Report the security status of ROSS AISs to the ISSO;
- Evaluate known vulnerabilities associated with their assigned area of technical responsibility to ascertain if additional safeguards are needed;
- Conduct periodic AIS security evaluations within their assigned area of technical responsibility to ensure compliance requirements;
- With the ISSO and Directorate Level TASO’s, ensure that users are aware of ROSS policies concerning unauthorized use of the AIS(s);
- With the ISSO and Directorate Level TASO’s , ensure that AIS users are not granted multiple user-IDs or multi-login capability to the ROSSe AIS, without specific exemption approved by the CSM;
- With the ISSO and Directorate Level TASO’s , ensure that the AIS(s) associated with their assigned area of technical responsibility are used only in a manner consistent with the ROSS policies contained herein and OMB Guidance;

- Support the AISSP development and maintenance process (See Section A-4.0);

A-4.0 SECURITY PLAN MAINTENANCE

The following describes the development/maintenance responsibilities for the ROSS Automated Information System Security Plan (AISSP):

- The ISSO for the ROSS AIS host facility is responsible for developing and maintaining the ROSS AISSP;
- The TASO's are responsible for ensuring that "as-is" configuration data is accurately recorded in AISSP annexes and are responsible for notifying the ISSO of all configuration changes;
- The TASO's will secure all necessary waivers and approvals prior to submitting their applicable AISSP configuration data annex, or AISSP annex changes, to the ISSO and the CSM for approval. The CSM will provide assistance in determining other waiver requirements;
- The ISSO will submit the final AISSP, or AISSP changes, to the CSM for review;
- The CSM will review AISSP submittals and forward them to the DAA for final accreditation;
- An individual AIS will not be operated until the approval process is completed and the DAA accredits the AIS's configuration data annex entry to the AISSP. Once the AIS is accredited, the ROSS ISSO is responsible for the implementation, operation and training in support of the of the AIS in a secure manner in accordance with OMB Guidance;

A-5.0 ACCESS CONTROL LIST RESPONSIBILITIES

To assure that only authorized users, with a need to know, are provided access to ROSS AISs, a formal process shall be implemented which will require the continuous cooperation of the CSM, OSM, ISSO, and TASO's. The formal process shall involve maintenance of a ROSS authorized user access control listing (ACL). The ACL shall be maintained in a manner that provides checks and balances, between the respective security managers' offices, against unauthorized/inadvertent tampering. The process shall, as a minimum, provide the following:

New AIS User Verification:

- Each Directorate Level TASO verifies the identity of all users requesting access;
- The Directorate Level TASO verifies user's "need to know" with pre-identified, authorized, functional area leads;
- The Directorate Level TASO verifies directly with OSM the security clearance / employment status of all users requesting access prior to allowing a user access to AISs;
- Each Directorate Level TASO coordinates with the ISSO to provide access to approved AIS users and to add approved user information to the authorized access control listings (ACL) for each respective AIS to which a user is granted access;

Periodic Maintenance:

- Each ISSO/ Directorate Level TASO will maintain up-to-date authorized access control listings (ACL) for the AIS or operations facility for which they are responsible. The ACL will log all additions, changes, or removals of user ACL entries, that may be caused by, but are not limited to: departures; deaths; additions; name changes; loss of security clearance; and or change in status of "need to know";
- The CSM, on a monthly basis, will collect from ISSO/ Directorate Level TASO's the regularly maintained ACL's for each AIS and forward the list to OSM, requesting security status verification;
- The OSM will supply the CSM with a verification of employee status information and assigned roles to support AIS user access grants, noting all discrepancies;
- The CSM will immediately inform ISSO/TASO's of discrepancies which impact existing AIS user access grants;
- Each TASO will immediately modify/revoke affected AIS user access grants, as required;

Instantaneous Response:

- The OSM will report immediately to the CSM any changes in an AIS user's clearance status, including temporary suspension or revocation of a clearance, that could necessitate their removal from the AIS;
- The CSM will evaluate the OSM change of security status notice and immediately inform ISSO/TASO's of required changes/revocations. A copy of the OSM notice, and CSM's conclusions, will be forwarded to the ISSO/TASO's;
- Each TASO will immediately modify/revoke affected AIS user access grants, as directed.