

The United States (U.S.) Army Land Warrior
Network (LandWarNet) Network
Operations (Network Operations) Architecture (LNA)
For
Public Key Infrastructure Management

Date of Issue: 8 April 2008

Date of Expiration/Suppression: Until Rescinded

Point of Contact:

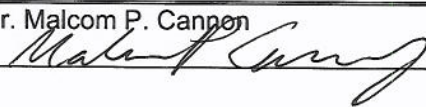
Enterprise NetOps Planning Division
NETCOM/9th Signal Command (Army)
ESTA-OSC&I-ENPD
Greely Hall, Building 61801
2133 Cushing Street
Fort Huachuca, Arizona 85613-7070
AENIA-Team@conus.army.mil

INTENTIONALLY LEFT BLANK

Status and Revision Record

Draft	Submitted By	Submitted To
3/19/2008	Will Lemons/Perot Systems/ESTA/ Enterprise Network Operations Planning Division	Lisa Barnett/Perot Systems/ESTA/Enterprise Network Operations Planning Division
4/8/2008	David A. Fox/NCI Information Systems, Inc./Enterprise Network Operations Planning Division	Malcom P. Cannon/ Government Technical Lead, Army LNA/ Enterprise Network Operations Planning Division

Change #	Description	Date	Name/Office of Person Entering Change
1.			
2.			
3.			
4.			
5.			

Approving Authority	Signature	Date
NETCOM-ESTA-OSC&I-Enterprise Network Operations Planning Division:	Mr. Malcom P. Cannon 	29 APR 08

INTENTIONALLY LEFT BLANK

Introduction

The following two tables are a summarization of information contained in the United States Army Land Warrior Network (LandWarNet) Network Operations (Network Operations) Architecture (LNA). They provide a summarization of the functions, interactions, and descriptions of a specific capability, as they are needed to operate, manage, and defend the LandWarNet. These tables are presented to assist the implementers, vendors, and other interested personnel to understand the operational activities and systems functions to help determine what is the most operationally and cost effective transition path to achieve Net-Centric operation and management of the LandWarNet.

Our LNA architects follow a process including a series of reviews to ensure the resulting architectural products are technically sound, result in an integrated Network Operations architecture, and exclude unnecessary duplication and/or stove piping.

This includes:

- Conducting research
- Reviewing Army and commercial vendor documentation
- Analyzing best operational concept, configuration, and any technical requirements/standards
- Staffing with SMEs and POCs

Once this process is completed and approved the information is entered into the LNA. Based on this approved information, these tables are then produced.

This table provides the Public Key Infrastructure Management interactions with other LNA capabilities. It also provides the names of the capabilities and the data exchanged (data elements). Definitions of the Data Elements are provided to help in the understanding of the data elements. All this information is contained in the architecture.

Table One – Public Key Infrastructure Management interactions with other capabilities

FROM	TO	DATA FLOW TEXT DESCRIPTION	DATA ELEMENTS	DATA ELEMENT DEFINITION
Defense Information Systems Command Certificate Authority - External	Public Key Infrastructure Management	Contains Key and certificate data sent from the External Source to the Public Key Infrastructure Management System.	Key Certificate Data	Key Certificate Data: Contains the Key and/or Certificate data used to validate users and systems that is part of the encryption process, as well as a validation of the status of the key or certificate.
High Assurance Internet Protocol Encryptor Management	Public Key Infrastructure Management	Contains data sent from the High Assurance Internet Protocol Encryptor Management system to the Public Key Infrastructure Management System.	Request for Data	Request for Data: This is a generic request for data from one Network Operations system to another. The type, content, format, and frequency of the data requested and/or sent is dependant on the respective unique systems.
Public Key Infrastructure Management	Defense Information Systems Command Certificate Authority - External	Contains request for data from the Public Key Infrastructure Management system to an external authority	Request for Data	Request for Data: This is a generic request for data from one Network Operations system to another. The type, content, format, and frequency of the data requested and/or sent is dependant on the respective unique systems.
Public Key Infrastructure Management	High Assurance Internet Protocol Encryptor Management	Contains Key/Certificate data sent from the Public Key Infrastructure Management system to the High Assurance Internet Protocol Encryptor Management System	Key Certificate Data	Key Certificate Data: Contains the Key and/or Certificate data used to validate users and systems that is part of the encryption process, as well as a validation of the status of the key or certificate.

This table provides the Public Key Infrastructure Management functions. It also provides the purpose of the function and indicates if it is a Key Performance Parameter (KPP). The Hierarchical Number is where in the architecture the information can be found.

If a function is designated as a KPP, a “Yes” will appear in the KPP column. All Priority One and Two functions are KPPs. If the function is designated as a KPP, it will have a justification otherwise “N/A” will be shown in the Justification column.

Priorities Definitions:

Priority One – Highest priority and is required.

Priority Two – Of lesser importance than priority one but still required.

Priority Three – This depicts functionality we are aware is available in the technology and it would be beneficial to have it but it is not required.

Priority Four – Use of this priority depicts functionality we would like to see in a product/vendor but realize that the technology may not be mature enough to support. Our desire here is to communicate to vendors the desired functionality.

Table Two – Public Key Infrastructure Management Functions and Key Performance Parameters

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Assign Privileges to Administrative Groups	The system shall provide the ability to assign privileges (read, write, execute, access to, restrictions from) to administrative groups. Administrative groups are composed of administrative accounts used to manage the platform.	This is needed for administrators to quickly and securely add and remove access permissions to management platforms.	2	Yes	1.1.2.3.3

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Configure Communication Resources	The system shall have configurable communication parameters. These parameters can be set between component-to- management consoles, manager-to-agent and manager-to-management consoles; client-to-server, client-to-client, Virtual Private Network Device-to-remote user, and server-to-server components. This includes configuring ports, Internet Protocol address.	This is needed to securely configure communication channels between agents and management platforms ensures secure transfer of data between the two elements.	1	Yes	1.1.4.6.1
Customize Knowledge Base	The system should enable administrators to customize its digital documents knowledge bases for its managed clients/agents/applications, and supported customers, organizations, or services. This enables administrators to add Army specific documents (approval to operate, tailored standard operating procedure/Tactics, Techniques, and Procedures, Army-refined Frequently Asked Questions, Intrusion Prevention System Policy/Behavior-Based Rule Implementation Instructions, Field Manuals/Behavior-Based Rules, etc.) to standard Enterprise documents and links within the knowledge base.	Not Applicable (N/A)	3	No	1.1.6.2.2
Define Access Privileges	The system shall enable designated administrators to define, and subsequently enforce access privileges for other administrators, users and assets to the management platform its data and any managed assets.	This is critical for securing LandWarNet resources and preventing unauthorized users from making changes that could lead to false alarms, failure of vital system functions, and corruption of data used to operate, manage and defend the LandWarNet.	2	Yes	1.2.2.5.4

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Detect and Report Login Credential Changes	The system shall identify when users/administrators have changed, or attempted to change, their login credentials (user name, password, domain) and report this change.	This is needed to track user activity and identify those types of activities that may indicate unauthorized changes to accounts.	2	Yes	1.1.2.4.1
Display Change History	The system shall display information regarding historical changes to the system and its managed objects or applications.	This is needed to enable administrators to verify authorized changes and identify unauthorized changes to the management system and any managed devices and applications.	1	Yes	1.1.1.4
Display Events	The system shall display dynamic near-real-time events based on alarm severity, time, hierarchical importance, client groups, etc. The system shall support drill down capabilities to display the underlying events behind larger alarms/incidents.	This is needed for the operation, maintenance, and defense of the Global Information Grid and LandWarNet.	1	Yes	1.1.1.12
Display Help	The system should provide the ability to view help files specific to the application or management system.	N/A	3	No	1.1.1.18
Display Knowledge Base Information	The system should display requested information from a particular knowledge base, in response to administrator queries. It should support information retrieval and display from authorized (administratively-linked) external knowledge bases (e.g., a vendor maintained knowledge base. This facilitates rapid trouble-shooting and insightful decision making, particularly by less experienced administrators.	N/A	3	No	1.1.1.19
Display Results of Diagnostics	The system shall present results of diagnostic routines executed on a network device.	This is needed to facilitate trouble shooting.	2	Yes	1.1.1.20

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Encrypt Data Exchanges	The system shall provide secure (encrypted) data exchange between a manager and clients. Certain types of data being exchanged require encryption (e.g., logon credentials). The system shall provide the capability to encrypt data transferred between the system and assets using Secure Socket Layer and Transport Layer Security that is Federal Information Processing Standards Publication 140-2 compliant.	Secures Network Operations management data used to control management platforms on the LandWarNet.	1	Yes	1.1.2.4.1
Manage Administrator Accounts	The system shall provide the ability to manage (add, modify, verify, delete) accounts that are used to administrate the system. This also includes the ability add and remove users from groups.	This is needed to ensure that access to management systems is controlled and secure.	2	Yes	1.2.2.3.1
Manage Component Grouping	The system shall allow administrators to define groups of assets. Groups may be created using different characteristics, including hierarchical, organizational, geographical, or functional (e.g., Email Servers). Also, the system shall enable administrators to assign specific assets/ components to defined groups.	This is needed to enable the administrators to perform common operations upon them (loading patches, signatures, profiles, access control list, etc.) - speeding implementation of security measures during an attack, reducing the chances of error, and reducing overall administrator workloads.	2	Yes	1.1.4.1
Manage Groups	The system shall manage (create, modify, delete) User Groups, with user roles and privileges. It shall support User Group creation, data entry/ modification, and deletion by authorized system users. This includes the ability to remove multiple groups/super groups (groups that	The system is critical to the operations and security of this Network Operations system and the LandWarNet. User accounts and their associated User Group(s) will be used throughout the Enterprise to control privilege-based access to various resources/assets and services, track trouble calls/service	1	Yes	1.1.2.6.2

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	contain other groups) within a single action.	requests, provide alerts/notifications, and to maintain audit/transaction logs (In accordance with Army Regulation 25-1 and Army Regulation 25-2).			
Perform Local Authentication	The system shall authenticate users, administrators, and assets from data stored locally within the management application or device.	This is needed for the authentication of users to access and resources on the LandWarNet and is required by Army Regulation 25-1, and Army Regulation 25-2.	1	Yes	1.1.2.5.1
Perform Operations on Multiple Assets	The system shall permit administrators to interact with multiple managed assets on a single screen. It allows them to select and perform operations on individual assets, and groups of assets (Hardware, Software, Agents), from administratively defined (pick) lists of available assets/asst groups and operations. The system shall enable the administrator to define and save groups of assets for future pick list displays (to perform future operations upon).	This is needed to save the administrators considerable time, enable central management and maintenance of large network - enhancing overall reliability and security.	2	Yes	1.1.2.1.1
Perform Remote Authentication	The system shall authenticate users, administrators, and assets from a remote authentication service on the network.	This is the core function for the authentication of users to access and resources on the LandWarNet and is required by Army Regulation 25-1, and Army Regulation 25-2.	1	Yes	1.1.2.5.2
Provide Administrator Audit Log	The system shall provide administrator audit log information, to include the administrator's identification, time stamp, the specific activity/transaction performed, changes in permissions, and any other specified data of interest related to administrator transactions on	This is required in accordance with Department of Defense Instruction 8500.2, Army Regulation 25-1 and Army Regulation 25-2.	2	Yes	1.1.2.4.10

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	the system.				
Provide Command Line Interface	The system shall use a command line interface for system or account administration locally and remotely.	This is needed to enable administrators to execute changes on large groups of configuration items via a single command.	2	Yes	1.1.1.6
Provide Command Line Interface and Application Program Interface Security	The system should provide security mechanisms for Command Line Interface and Application Program Interface access to the system. The system should enforce security for command line input that is functionally identical to graphical user interface access restrictions and controls; security for Advanced Programming Interfaces that are functionally identical to graphical user interface access restrictions and controls.	N/A	3	No	1.1.2.4.8
Provide Communication Ports Security	The system shall provide the capability to designate a limited set of ports for communication between management platforms and managed components.	This is necessary to configure management platforms to communicate across routers and switches (considering port restrictions that may be applied to network devices) within the LandWarNet.	1	Yes	1.1.2.4.2
Provide Defineable Report Filters	The system should provide filters that can be created and modified. Filters provide a way to produce reports that provide data on a specific attribute(s).	N/A	3	No	1.1.3.6.18
Provide Device and Media Configuration Information Repository	The system shall store all configuration information about devices and media that is generated by the management system or its sub-systems/agents, to include any unique communications/ encryption settings. This also includes new/staged, current, and multiple copies of historical configuration data.	This is needed to maintain and defend LandWarNet systems via their configurations. It supports restoring and reconstitution of vital assets and applications.	2	Yes	1.1.1.2.1

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Provide Event Log Reports	The system shall produce reports containing event and associated user activity logs.	This is needed to meet Army Regulation requirements for reporting on potential security breaches.	2	Yes	1.1.3.6.21
Provide Frequently Asked Questions Feature	The system should support a Frequently Asked Question capability, providing searchable, quick solutions for common problems for both administrators and customers/users.	N/A	3	No	1.1.6.1.1
Provide Graphical Interface	The system shall provide a graphical user interface enabling users and/or administrators to access and operate the system from their terminal or via a web-accessible Interface. The system functionality should be the same whether the operator accesses the system via the terminal or at the server/system's native interface.	This is needed to simplify the use of the management system.	2	Yes	1.1.1.7
Provide Help Feature	The system should provide help functionality. This can be an on-line functionality or provided locally on the platform. It should provide a search and index capability.	N/A	3	No	1.1.6.1.2
Provide Import Digital Documents For Knowledge Bases	The system should import vendor supplied Digital Documentation Knowledge Base information.	N/A	3	No	1.1.6.2.4
Provide Knowledge Base	The system should provide a knowledge base. Knowledge bases are searchable (via queries) repository of information about a specific topic or product. The knowledge base should contain at a minimum; frequently asked questions, trouble-shooting wizards, Uniform Resource Locator's for additional help/information.	N/A	3	No	1.1.6.2.1

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Provide Knowledge Base Repository	The system should store Network Operations Knowledge Base information. This includes all information stored in the Knowledge Base used primarily by administrators in the operations and maintenance of systems and services.	This is essential for the basic operation of the Network Operations Systems Knowledge Base management capabilities.	3	No	1.1.5.2
Provide Multiple Component Access Controls	The system shall control the administrator's ability to only perform operations to those assets/asset groups they are authorized to manage.	This is needed to enable automated administrative access controls - enhancing overall reliability and security.	2	Yes	1.1.2.1.3
Provide Operational Reports	The system shall provide operational Network Operations reports, to include those on component and aggregated asset/system utilization (or usage); failed components/assets; configuration settings for all/designated components/assets; and asset/device/storage information.	This is needed to allow the element manager to combine and summarize device/storage information, Job Status, Job Volume, Device Utilization, media verification, job failures, job schedules, report alerts.	2	Yes	1.1.3.6.12
Provide Predefined Display Formats	The system shall display predefined formats/displays to make the system usable immediately after the initial installation.	This is needed for basic operation of the system out of the box, reducing configuration and implementation time.	2	Yes	1.1.1.8
Provide Predefined Reporting Filters	The system should display filters to reduce displayed data based on relevancy and provide predefined display filters to support analysis of reported data.	N/A	3	No	1.1.3.6.20
Provide Public Key Infrastructure/X.500 Management	Public Key Infrastructure provides a method for secure communications over networks. The Department of Defense Public Key Infrastructure is not an application that is contained by Active Directory. It is its own	This is necessary for the authentication of users to the Active Directory environment.	1	Yes	1.1.5.13.1.6

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	<p>infrastructure, which can function on top of Active Directory environment. The Department of Defense Public Key Infrastructure is its own infrastructure separate from Active Directory, but from an operational standpoint, Active Directory does store the X.509 certificates used in Department of Defense Public Key Infrastructure within the Directory Service. This will require maintenance of the certificates within the directory.</p>				
Provide Remote Administration	The system shall provide secure, Internet protocol-based remote administration of the manager and its managed assets.	This is required to secure the LandWarNet and operate large networks.	2	Yes	1.1.2.1.4
Provide Single Component Access	The system shall enable administrators to interact with a single monitored asset or service on a single screen. This includes enabling them to view and manipulate the asset/service's status, type, capacity, utilization, allocation, and location.	This is needed to facilitate defensive actions, maintenance, and operational management of core components and services underpinning the entire LandWarNet.	2	Yes	1.1.2.1.2
Provide Standard and Predefined Reports	The system should predefined/ standard reports and views. The system should also provide graphics within text reports (e.g., Trending Reports may contain pie charts, bar charts, line charts and other standard graphics). The system should publish reports in Hyper Text Markup Language eXtensible Markup Language, Sequential Query Language, American Standard Code for Information Interchange, Joint	N/A	3	No	1.1.3.6.10

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	<p>Photographic Experts Group and other standard languages/ formats; be able to print and email all generated reports. The system should be able to provide displays and reports on all on the following:</p> <ul style="list-style-type: none"> a) audit reports that detail modifications and upgrades to the system b) identifying all major problems (per pre-defined service level agreement/service support program, per period) c) resolution time for incidents/problems d) closed incidents/problems e) problems that result in the highest percentage of resource utilization f) first contact to closure for incidents or problems g) first call closure for incidents or problems h) open incidents or problems i) incidents or problems that violate service level agreement/service support program, Service Level Indicators j) closed incidents and problems k) resolved incidents and problems l) escalated incidents and problems m) based on each individual support staff for the number of incidents or problems that they turned over to other support staff during a shift change n) based on department/group for the number of incidents or problems that are turned over to other support staff 				

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	<p>during a shift change</p> <p>o) trends by agent/support staff for number of incidents and problems opened per day, week, and month</p> <p>p) trends by agent/support staff for number of incidents and problems resolved per day, week, and month</p> <p>q) trends by agent/support staff for number of incidents and problems escalated per day, week, and month</p> <p>r) trends by agent/support staff on the average time taken for incidents and problems to move from open to resolved status</p> <p>s) trends by agent/support staff on the average time spent talking to customers/ users regarding an incident or problem</p> <p>t) trends by agent/support staff on percent of first contact to resolution regarding incidents and problems</p> <p>u) trends (daily, weekly, monthly) by agent/support staff on percent of first call resolution regarding incidents and problems</p> <p>v) trends (daily, weekly, monthly) by agent/support staff on the average first contact to resolution regarding incidents and problems</p> <p>w) trends (daily, weekly, monthly) by agent/support staff on the average first call to resolution regarding incidents and problems</p> <p>x) trends by group/department for number of incidents and problems opened per day, week, and month</p>				

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	<p>y) trends by group/department for number of incidents and problems resolved per day, week, and month</p> <p>z) trends by group/department for number of incidents and problems escalated per day, week, and month</p> <p>aa) trends by group/department on the average time taken for incidents and problems to move from open to resolved status</p> <p>bb) trends by group/department on the average time spent talking to customers/ users regarding an incident or problem</p> <p>cc) trends by group/department on percent of first contact to resolution regarding incidents and problems</p> <p>dd) trends by group/department on percent of first call to resolution regarding incidents and problems</p> <p>ee) trends by group/department on the average first contact to resolution regarding incidents and problems</p> <p>ff) trends (daily, weekly, monthly) by group on the average first call to resolution regarding incidents and problems</p> <p>gg) Incident/Problem rollups by LandWarNet Command, Control, Communications, Computers, and Information Management/Information Technology service or product</p> <p>hh) Users that access a specific asset</p> <p>ii) users that own a specific asset</p> <p>jj) operational assets which have exceeded their life cycle (to identify</p>				

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	<p>equipment that needs to be replaced)</p> <p>kk) minimum, maximum, and averages for all time and numeric based reports</p> <p>ll) number of users that access a defined service</p> <p>mm) customers and their associated users</p> <p>nn) specify the concentration and distribution of vendors and their related products within the enterprise (allows the organization to more clearly understand the impact of issues related to specific products or vendors)</p> <p>oo) life cycle plans (projections) for an asset</p> <p>pp) service or product defect status</p> <p>qq) service or product enhancement request/Request For Change reports.</p>				
Provide System Documentation	The system should support documentation for a specific technology/capabilities. This includes system design, implementation and user guides.	N/A	3	No	1.1.6.2.3
Provide User Account Repository	The system shall store user and administrator account information for the management system.	This is needed to control access to the management system and to support addressing for notification messages/alerts.	2	Yes	1.1.1.2.7
Provide User Activity Log	The system shall create and manage the User Activity (Audit) Log, recording all user transactions, and changes to permissions on the system in accordance with Army Regulation 25-2.	This is required per Army Regulatory requirements and provides a means to verify Network Operations staff actions, conduct rollbacks, and conduct post-mortems/after-action-reviews to improve Network Operations procedures.	1	Yes	1.1.2.4.9

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Provide User Defined Display Filters	The system shall enable administrators to define filtering criteria to view a subset of the available information.	This is needed to enable administrators to quickly view all data based upon specific criteria, facilitating analyses, troubleshooting, work scheduling, etc.	2	Yes	1.1.1.11
Provide User Defined Display Formats	The system should allow users to create, add, modify, or delete display formats.	N/A	3	No	1.1.1.10
Provide User Defined Report Format	The system should allow for defined presentation formats to view available information. It should enable the customization of the fields in a report template or system-provided default report. The system should provide report creation tools and support ability to customize reports. The system should enable the user to define output report formats in Extensible Markup Language, Hypertext Transfer Protocol, American Standard Code for Information Interchange, Sequential Query Language, and American Joint Photographic Experts Group.	N/A	3	No	1.1.3.6.19
Provide User Log Data Repository	The system shall store User Activity Log data collected for analyses by the management system.	This is needed to trace user logon activity and to meet Army Regulation 25-1 and Army Regulation 25-2 requirements (punitive requirement).	1	Yes	1.1.4.1
Provide Web Accessible Display	The system shall interact with devices via a web based interface. The functionality shall be equivalent to the capability provided by non-web based user interfaces.	This is needed to support Army requirements to provide web accessible interface.	2	Yes	1.1.1.17
Receive Certificate	The system shall receive the actual key or certificate that was sent by the Send Certificate function from the Defense	This provides keys needed to access the assets on the LandWarNet.	1	Yes	1.1.5.6.7.9

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	Information Systems Command certification authority.				
Receive Certificate Request	The system shall receive the request for a key or certificate to be generated.	This is the first step in gaining a certificate that provides authentication, encryption, and non-repudiation, and is required to access assets on the LandWarNet.	1	Yes	1.1.5.6.7.8
Receive Certificate Revocation Request	The system shall receive the information necessary to revoke a certificate by the request of the Send Certificate Revocation Request system function.	This ensures that certificates that have been revoked cannot continue to be used to access the LandWarNet, to decrypt emails, or to provide non-repudiation.	1	Yes	1.1.5.6.7.4
Receive Certificate Revoked Notification	The system shall receive the completion notification from a previous request that a key or certificate should be revoked has been completed.	This is necessary to ensure that compromised certificates have been revoked.	1	Yes	1.1.5.6.7.6
Receive Certificate Status Data	The system shall Receive Certificate Status Data (certificate revocation lists) on the Online Certificate Status Protocol Requestor and receives the Key or Certificate Status Data sent from the Online Certificate Status Protocol Responder. The Online Certificate Status Protocol Requestor returns the good, revoked or unknown status back to the Public Key Infrastructure enabled application.	This is needed to validate that a certificate provided has not been revoked.	1	Yes	1.1.5.6.7.10
Receive Certificate Validation Request	The system shall receive the request to validate a key or certificate. This would be running on an Online Certificate Status Protocol Responder checking the data sent from an Online Certificate Status Protocol Requestor.	This enables the validation of a certificate.	1	Yes	1.1.5.6.7.7

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Receive Events in Standard Protocols	The system shall receive events via industry standard protocols (Storage Management Initiative - Specifications, Simple Network Management Protocol v2/3, common information model, Extensible Markup Language, User Datagram Protocol, etc.)	This is needed to reduce the amount of time spent integrating products.	2	Yes	1.1.5.1.1.1.1.3
Report Inactive Administrator Accounts	The system shall detect and report inactive administrator accounts. Inactive administrators are those who have not accessed a specific system for a predefined amount of time. Inactive administrators shall be flagged for administrative attention and possible action (i.e., account suspension, deletion, etc.). The system shall provide alert and report mechanisms to system administrators to act on flagged files.	This is needed for enforcing secure access controls over the Network Operations systems used to secure, operate, and manage the LandWarNet and its supported Army and Business systems.	2	Yes	1.1.2.3.2
Reset Administrator Account Parameters	The system shall establish the capabilities expected from a Manager to reset Administrator Account/Group parameters of an application. A reset is the ability to lock or unlock, make active or disable, or change any of the settings of an account.	This is to provide the ability to lock accounts and unlock administrative accounts allowing for the securing of the LandWarNet.	2	Yes	1.1.2.3.4
Schedule the Production of Reports	The system should support the ability schedule the production of reports. Scheduling will allow for monthly, daily, and hourly configuration such that reports can be run automatically.	N/A	3	No	1.1.3.6.6

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
Send Certificate	The system shall send the actual keys and certificates that were generated to the Receive Certificate function from the Defense Information Systems Command certification authority.	This is necessary to provide certificates to log on to any LandWarNet asset.	1	Yes	1.1.5.6.6.8.2
Send Certificate Request	The system shall send a request for a key or certificate to be generated under the control of the certification authority.	This is necessary to obtain certificates to log on to any LandWarNet asset.	1	Yes	1.1.5.6.6.8.1
Send Certificate Revocation Request	The systems should send the data necessary to request that a particular key or certificate be revoked.	This ensures that certificates or keys that have been compromised are revoked.	1	Yes	1.1.5.6.6.8.5
Send Certificate Revoked Notification	The system should send the notification back to the requestor: the key or certificate was revoked at their request.	This is necessary to ensure the non-repudiation of a LandWarNet user.	1	Yes	1.1.5.6.6.8.4
Send Certificate Status Data	The Send Certificate Status Data system function is running on the Online Certificate Status Protocol Responder and sends the Key or Certificate Status Data back to the receiving Online Certificate Status Protocol Requestor. The status is good, revoked, or unknown. This is determined from the passport that was sent to the Online Certificate Status Protocol Responder from the Real Time Certificate Authority system.	This is necessary to determine the status of certificate data.	1	Yes	1.1.5.6.6.8.3
Send Certificate Validation Request	This system function sends the request to validate a key or certificate. This would be a Public Key Infrastructure enabled application sending out a request that an Online Certificate Status Protocol Requestor would pick up and send the data to be checked by	This is necessary for validation of keys or certificates.	1	Yes	1.1.5.6.6.8.6

Name	Purpose	Justification	Priority	Key Performance Parameter	Hierarchical Number
	the Online Certificate Status Protocol Responder.				
Send Incident/Problem Data	The system shall transmit Incident and Problem data. The system shall, upon triggering of operational or security related problems, send or transmit the data (time of event, Internet Protocol address, category of event, etc.) needed to create a workflow record.	This is necessary for ensuring that assets in the LandWarNet are operating optimally.	1	Yes	1.1.5.6.6.4
Support Multiple Concurrent Administrators	The system shall support multiple administrators performing management operations concurrently.	This is needed to support the ability for multiple administrators to perform operations concurrently reducing the total cost of ownership.	2	Yes	1.1.2.2
Track Logon Attempts	The system shall detect and log user logon attempts (successful or otherwise). The system shall provide alerts/reports to system administrators to act on multiple failed attempts.	This is needed for enforcing Army Regulation 25-1 and Army Regulation 25-2 security regulations and enforcing secure access controls over the systems used to secure, operate, and manage the LandWarNet and its supported Army and Business systems. It also supports post-mortems on Information Technology outages/attacks.	1	Yes	1.1.2.4.2

This Glossary provides the “To” and “From” Interactions with other Capabilities Glossary (Reference Table One). This glossary is generic to the Land Warrior Network (LandWarNet) Network Operations (Network Operations) Architecture (LNA) therefore some items will be contained in the Glossary that are not in this document.

Interactions with other Capabilities Glossary

Active Directory: This system configures, manages and monitors quality of service of the Army’s Active Directory infrastructure. Fully leverages the Army’s Lightweight Directory Access Protocol/X.500 and Public Key Infrastructure services. Provides features to detect and resolve/manage critical conflicting updates between Active Directory managed objects, to include Active Directory/Lightweight Directory Access Protocol Schema changes, Domain names, NT Domain emulation, Security Identifier assignments, and group membership/controls. Manages Active Directory forests, the global catalog, directory replication across domain controllers, implementation of Public Key Infrastructure certificates (to encrypt directory data), Active Directory Trust relationships, and group policies (which control Active Directory objects/users’ access to other Active Directory objects - applications, application settings, roaming user profiles, and user data - from any managed computer). Also provides health/security monitoring, troubleshooting and other tools. Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides Active Directory inventory, configurations and events/incidents to Configuration Management Database/Service Support.

Active Directory Services Management: Provides standard configuration, management and quality of service monitoring of the Army’s Active Directory infrastructure (which helps name, describe, locate, access, manage, and secure information about available network resources and users). Fully leverages Lightweight Directory Access Protocol/X.500 and Public Key Infrastructure services. Provides features to detect and resolve/manage critical conflicting updates between Active Directory managed objects, to include Active Directory/Lightweight Directory Access Protocol schema changes, domain names, NT Domain emulation, assignment of Security Identifiers, and group membership management. Manages Active Directory forests, the global catalog, directory replication across domain controllers, implementation of Public Key Infrastructure certificates (to encrypt directory data), Active Directory Trust relationships, and group policies (which control Active Directory objects/users’ access to other Active Directory objects - applications, application settings, roaming user profiles, and user data - from any managed computer). Also provides Active Directory health/security monitoring, Capacity, Availability, and Performance/utilization metrics, event reporting, troubleshooting and other supporting functions/tools.

Anti-Virus Management System: An enterprise-level management system, and clients and agents that manage the configuration and actions of the anti-virus/SPAM/spyware system mounted on a computing host. Aggregates agents and managers reports and events for analysis and troubleshooting. Provides protection to

hosts based upon commercially provided signatures. Provides Anti-Virus security events/incidents to Security Information Management System; operational events/incidents, Anti-Virus inventories and configuration to Configuration Management Database/Service Support; requests and retrieves updates from authorized external sources (e.g., Vendor web site or Area Processing Center). Relies on System Management System, Security Configuration Remediation Management and other systems to disseminate agents to client hosts and to maintain Anti-Virus management system's server.

Backup and Recovery Management: This system enables end-users and administrators to schedule and manage data backup and/or data recovery (restoration) for computing platforms. Configures, manages and controls backup media and any agents. Able to leverage other storage devices on the network (e.g., Network Attached Storage or Storage Area Network) – but may not manage or control all of those disks. Supports defining specific/custom backup jobs as a set of files by name, schedule, and mode (disruptive or non-disruptive). Supports differential backups (only files modified since the last backup is archived) and partial recovery (e.g., to rollback the host to a specific date/time following a failed patch). Provides notice and time for backups to users, so they can either log off, standby, or close certain application programs until the job is fully executed. Provides system events/incidents, system/agent inventories and configuration to Configuration Management Database/Service Support. Relies on other Network Operations systems for the system's configuration, defense and to mount/update any agents on hosts.

Capacity, Availability, and Performance Monitoring System: This system collects, processes, analyzes, stores, and reports metrics data about the capacity, availability and performance of Internet Protocol network components, selected Command, Control, Communications, Computers, and Information Management/Information Technology services (e.g., storage services/Active Directory), and staff. Capacity metrics include transmission bandwidth/rates, central processing unit utilization, disk usage, disk/RAM/ Queue size, transactions per second, etc. Availability metrics include component mean time between failures, time in service as scheduled, mean time to repair/serviceability measures, etc. Performance metrics include transaction times (e.g., to authenticate a user/send an email), the number of threat signatures/attacks detected, the number of Trouble Ticket/Work Units relating to security events, number of re-opened Trouble Ticket/Work units, Bit-error-rates, Jitter rates, customer survey satisfaction/ complaint rates, etc. Enables the user to define component-focused models used to aggregate and calculate Capacity, Availability, and Performance metrics for reporting. Requests and processes Capacity, Availability, and Performance Data from Configuration Management Database/Service Support, and other Network Operations Managers/Element Managers.

Collaboration Management: This system configures, manages and assures the availability and performance of the Army's Collaboration service (voice, video, conferencing, document and application sharing, instant messaging, and whiteboard functionality). Provides provisioning/subscription management, session management/

monitoring, traffic analysis, capacity/utilization metrics, infrastructure-based modeling, Capacity, Availability, and Performance/Event reporting, troubleshooting and other supporting functions/tools. Also supports Collaboration-related Anti-Virus, Anti-SPAM, and Backup and Recovery solutions, when necessary (e.g., can use proprietary components when existing Network Operations solution is incompatible). Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/ schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support.

Configuration Management Database/Service Support: The Configuration Management Data Base/Service Support system provides overarching Enterprise management through Service Desk/workflow management capabilities. Integrates Service Desk features with Incident/Problem Management, Change Management, Asset Management, Release/Project Management and Configuration Management components into a single system to support the operations of an Information Technology Infrastructure Library® Service Desk process. The system provides an integrated view of all aspects of incidents, problems, assets, services and customers. Its' Configuration Management Database repository is the authoritative source for data related to customers, users, assets, and services, providing a single location for all Information Technology management data and a single access point for a consolidated view of all Information Technology assets and users. Uses peer-to-peer and hierarchical interactions to form a distributed infrastructure to operate, manage and defend the LandWarNet's infrastructure/ Information Technology staffs.

Cryptographic Management: Cryptographic Security Services are measures and controls taken to deny unauthorized persons information derived from telecommunications and ensure the authenticity of such telecommunications. The scope of this architecture includes only the Network Operations portion of the Cryptographic Security Services capability, namely crypto security – which consists of: Access Control (Registration, Enrollment and Privileging); Product/Service Requests, Generation, Ordering and Distribution; and Tracking and Accountability.

Data Security at Rest: An enterprise-level management system that configures and manages the actions of data encryption software/devices for stored/archived data; aggregates their reports/events for analysis/troubleshooting. Provides ability to manage, archive and restore encryption keys for the encryption software/devices; supports transitioning of designated keys/data associated to deploying units to a designated peer/hierarchical Network Operations organization in the gaining Theater.

Database Element Manager: This system configures and manages different types of large, enterprise-application level databases (Oracle, MS SQL, Sybase, Informix, etc.; may have separate manager per vendor). Specifically provides threshold/parameters-based monitoring/alarms, user/group access control mechanisms, data access controls/strategy, database mirroring (Continuity of Operations +), event/scheduled reporting, and database configuration management (schema management,

normalization, and de-confliction. Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support. Database servers' hardware and Operating System software are supported and maintained by existing Land Warrior Network (LandWarNet) Network Operations Architecture capabilities such as: Systems Management, Anti-Virus, Host Intrusion Detection System/Host Intrusion Prevention System, Back-up and Recovery, etc.

Email Management: The Email Service Management Capability configures, manages, and assures the availability and performance of the Army's Email service. Provides email provisioning/subscription management, event monitoring, traffic analysis, capacity/use (Capacity, Availability, and Performance) metrics, infrastructure-based modeling, Event/Capacity, Availability, and Performance reporting, troubleshooting and other supporting functions/tools. Also supports Email Anti-Virus, Anti-SPAM, Backup and Recovery, and other solutions, when necessary (e.g., can use proprietary components when existing Network Operations solution is incompatible). Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support.

Firewall Element Manager: The Firewall Element Manager configures and manages Firewall devices; includes configuration of ports, interfaces, Network Address Translation/Port Address Translation tables, Domain Name System services, Virtual Private Network handling rules/policies, traffic scanning/packet inspection rules, threat/packet state signatures/profiles, and traffic blocking/Alert rules/policies/profiles. Firewall Element Manager receives and applies firewall configuration profiles to managed firewalls; provides firewall Events/Simple Network Management Protocol Traps, firewall inventories, firewall configuration data to Internet Protocol Network Management System. Enables Firewall Element Manager users to access and operate the Internet Protocol Network Management System remotely.

Frequency Spectrum Management: The Spectrum Management capabilities include all items necessary to make a valid frequency assignment to all emitters in the area of responsibility. These support system certification to verify that compliant equipment is being used, topographic management of the terrain data, data exchange in the client/server environment, compliance of the frequency records, interference analysis and reporting for frequency allocations, Joint Restricted Frequency List coordination, Electronic Warfare de-confliction to assess a planned Electronic Attack, and Allotment Plan Generation.

High Assurance Internet Protocol Encryptor Management: The High Assurance Internet Protocol Encryptor Manager configures and manages High Assurance Internet Protocol Encryptor infrastructure (e.g., Internet Protocol Inline Encryptors) employed within the LandWarNet. Features include setting High Assurance Internet Protocol

Encryptor authority, policy, configuration, inventory, and managing High Assurance Internet Protocol Encryptor Communications Security/encryption keys. High Assurance Internet Protocol Encryptor devices can be managed locally or remotely from a security management workstation using a common Management Information Base that enables disparate products to be configured via a common interface and protocol. High Assurance Internet Protocol Encryptors will also be able to receive software and firmware updates over the network in addition to policy changes. Provides High Assurance Internet Protocol Encryptor/Manager events/incidents, inventory, and configurations to Configuration Management Data Base/Service Support. Provides High Assurance Internet Protocol Encryptor Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager.

Host Based Security System: The Department of Defense's Host Based Security System secures general-purpose computing platforms from computer network attacks. It consists of a central management server/console, Host Based Security System repositories/scanners, Host Based Security System agents, and an authorized external knowledge base/repository. It brings today's firewall, host intrusion prevention, Anti-Virus, and Anti-Spy-ware software under a single agent's and central console's control. The central console baselines and subsequently scans platforms reconnecting or remotely accessing the network to block/remove hidden software (e.g., hackers' root kits/spyware) and other unauthorized modifications. Host Based Security System also has optional Network and Data Access Control extensions to enable remote updates and prevent unauthorized data release/leakages (e.g., classified data in Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) records/email). Its signature-based defenses against known attacks, coupled with generic unauthorized-behavior-based defenses against unknown (zero-day) threats, substantially reduces Computer Network Attack threats, while giving time to develop, test and field security patches. It enables tailored defenses and data access controls for critical (non-Commercial-off-the-Shelf) War-fighting and Business applications.

Host Intrusion Detection System: The Host Intrusion Detection System provides the capability for an agent to monitor host activities and identify those activities that have been identified as being potentially hostile. The potentially hostile activities are reported to a management console for analysis. Provides the same basic features as Host Intrusion Prevention System – except agents cannot block attacks. No longer supported by most Commercial-off-the-Shelf vendors; being phased out.

Host Intrusion Prevention System: The Host Intrusion Prevention System configures and manages host-mounted agents to monitor protected hosts' activities to identify and block unauthorized activities (using threat signature-based remedial/blocking rules). Identifies and/or mitigated potentially hostile activities are reported to a Host Intrusion Prevention System management console for analysis/troubleshooting. Console enables users to optimally configure a Host Intrusion Prevention System agent to match a host's applications suite and to tailor commercially (e.g., Common Vulnerabilities and Exposures) derived threat signatures/attack profiles and associated Agent blocking responses/alarms to address unique Army systems (e.g., Army Battle Command

Systems). Provides security events/incidents to Security Information Management System; operation events/incidents, Anti-Virus inventories and configurations to Configuration Management Database/Service Support; requests and retrieves updates from authorized external sources. Relies on System Management System, Security Configuration Remediation Management and other systems to disseminate agents to maintain Anti-Virus management console; may also do so to mount agents on Hosts (later configured by the Host Intrusion Prevention System console).

Identity Management: Identity Management is a centrally controlled enterprise capability used at all echelons (via standard policy enforcement points that leverage Army Knowledge Online, Common-Access-Card, Active Directory, Defense Information Systems Agency, etc.) to manage LandWarNet's Identification, Authentication, and Authorization services/functions. Permits only users, components/devices and applications with the proper/verified credentials (as defined by the information provider) to access information or services on the LandWarNet or Global Information Grid. Interacts with Defense Information Systems Agency and approved Commercial certificate registries to obtain validated certificates. Relies on other Network Operations systems (e.g., Internet Protocol Network Management System and System Management System) for its own configuration, software/operating system updates, and defense.

Information Assurance Vulnerability Management Compliance Manager: The Information Assurance Vulnerability Management Compliance Manager provides the capability to define configuration and software base line requirements for various systems types. The system then performs Information Assurance Vulnerability Management compliance scans of network, computing and some telecommunications devices – and groups of devices. Provides Vulnerability data to Security Configuration Remediation Management (for remediation); Provides security-related events to Security Information Management System; provides Scanner/Vulnerable Asset events/incidents, inventories and configuration data to Configuration Management Database/Service Support; provides Scanner Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager. NOTE - Requires adjustments to Firewall Element Manager/Network Intrusion Prevention System/Network Intrusion Detection System/Host Intrusion Prevention System/Host Intrusion Detection System configurations to prevent false alarms during scans.

Internet Protocol Network Management System: The Internet Protocol Network Manager is the primary network management system; manages/leverages sub-managers to control networked devices. Provides network-based discovery, Internet Protocol inventory management, mapping/display, event/Simple Network Management Protocol Trap processing, failure detection, isolation and analysis. Based upon sub-manager's reporting/remote entries, provides aggregated Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager; network inventory, device configurations, events/incident/status reports, and Requests for Trouble Ticket Status polls to Configuration Management Data Base/Service Support; network events/status data and topology to Network Common Operational Picture;

network inventory, device configurations, and topology to Policy-Based Internet Protocol Network Management. Supports peer-to-peer and hierarchical implementations.

Internet Protocol Network Vulnerability Scanner: The Internet Protocol Network Vulnerability Scanner performs vulnerability and security exposure scans of network, computing and selected telecommunications devices – and groups of devices; includes deep, non- Information Assurance Vulnerability Management scans. Able to define a number of different scanning profiles, based upon compliance baselines set in the compliance manager. It then interrogates systems using a number of different means/profiles to determine how vulnerable the system is to the scanning criteria. Provides Vulnerability data to Security Configuration Remediation Management (for remediation); provides security-related events to Security Information Management System; provides Scanner/Vulnerable Asset events/incidents, inventories and configuration data to Configuration Management Data Base/Service Support; provides Scanner Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager. Requires adjustments to Firewall Element Manager/Network Intrusion Prevention System/Network Intrusion Detection System/Host Intrusion Prevention System/Host Intrusion Detection System configurations to prevent false alarms during scans.

Layer 2 Switch Element Manager: The Layer 2 Switch Element Manager configures and manages Open Systems Interconnection (data-link) Layer-2 switching for a specific vendor's switches; includes configuration of Virtual Local Area Network, filtering/forwarding rules/profiles, spanning Tree Protocols, etc. Performs Internet Protocol device/MAC-level inventory/identification reporting. Receives and applies policy-based configuration profiles/rules to managed switches; provides Switch Events/Simple Network Management Protocol Traps, switch and Internet Protocol device inventories, switch configuration data to Internet Protocol Network Management System. Enables Layer 2 Switch Element Manager users to remotely operate the Internet Protocol Network Management System.

Layer 4 Switch Element Manager: The Layer 4 Switch Element Manager configures and manages Open Systems Interconnection (Transport) Layer-4 switching (capable of routing, switching and load-balancing Internet Protocol traffic) for a specific vendor's transport/backbone switches; Includes configuration of routing/switching protocols, load balancing protocols and policies, Access Control Lists, etc). Receives and applies configuration profiles to managed switches; provides Switch Events/Simple Network Management Protocol Traps, Switch and Internet Protocol device inventories, switch configuration data to Internet Protocol Network Management System. Enables Layer 4 Switch Element Manager users to remotely operate the Internet Protocol Network Management System.

Lightweight Directory Access Protocol/X.500 Directory Management: This system configures, manages and assures the availability and performance of the Army's Lightweight Directory Address Protocol/X.500 Directory services (directories for people, passwords, applications, Public Key Infrastructure certificates, and email/collaboration/

global address lists). Provides schema configuration management, directory partition management, index configuration (set attributes to index to support searches), directory data integrity checks, directory health/security monitoring, directory Capacity, Availability, and Performance/utilization metrics, event/Capacity, Availability, and Performance reporting, troubleshooting and other supporting functions/tools. Also supports Backup and Recovery solutions, when necessary (e.g., uses proprietary fix when existing Network Operations solution is incompatible/less optimal). Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support.

Meta-Directory Element Manager: In addition to providing the same email service management features noted above (Email underpins Defense Message System-Army), this system enables users to configure and manage unique X.500 Directory variations required to support official Department of Defense Message traffic over Army Radio Frequency and Internet Protocol networks. This includes Defense Message System-Army: 1) Message Transfer Agents; 2) User Agents; 3) Mail List Agents; 4) Directory System Agents; 5) Administrative Directory User Agents; 6) Directory User Agents; 7) Certification Authority Workstations. Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support.

Network Access Control: Enables remote/local configuration and management of Network Access Control servers to control Internet Protocol devices access to the LandWarNet. Allows authorized administrators to configure Network Access Control server rules and manage subsequent Internet Protocol device scanning for compliance to network policies/requirements. Places non-compliant systems into a Quarantine and Remediation Virtual Local Area Networks until corrective action is taken.

Network Attached Storage Element Manager: The Network Attached Storage Element Manager configures and manages network-attached storage devices (locally and remotely) from a central manager, with the help of agents. Enables users to configure access controls to drives/directories, partition/maintain drives, and provide threshold-based alarms/reporting. Provides operational events/incidents, Network Attached Storage inventories and configurations to Configuration Management Database/Service Support; sends Network Attached Storage devices' Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager.

Network Intrusion Detection System: The Network Intrusion Detection System provides the capability for an agent or device to monitor network traffic, identify that traffic that has been identified as being potentially hostile and report it to a central management console for analysis. The Network Intrusion Detection System's manager component configures and manages Network Intrusion Detection System sensors (which are not advertised to network/ Internet Protocol Network Management System

+) Provides software updates, configuration and management of Network Intrusion Detection System sensors, threat (Common Vulnerabilities and Exposures identifiers and custom) signatures, alarm rules/profiles; supports intrusion detection analysis. Provides Network Intrusion Detection System inventory, configuration, and Event/Incident status data to Configuration Management Database/Service Support; security events to Security Information Management System. Network Intrusion Detection System enables low-cost Global Information Grid/LandWarNet Sensor Grid within theaters/ posts/tactical networks.

Network Intrusion Prevention System: The Network Intrusion Prevention System configures and manages Network Intrusion Prevention System sensors; similar to Network Intrusion Detection System design and use – but adds ability to configure and manage suspect/malicious traffic blocking/attack mitigation rules/profiles (rules must pass authorized scans and software patches/updates).

Network Situational Awareness (Network Common Operational Picture (NETCOP)): The Network Common Operational Picture provides end-users with a near-real-time view of network situational awareness, with an emphasis on user-tailored graphical views of information technology assets, Incidents, Problems, and their status. Users may drill down into the information presented to see specific detailed information (from Configuration Management Database). Peer-to-peer/hierarchical links enable streamlined Network Common Operational Picture displays and reporting. Receives and displays Asset, Incident and Problem Data from the Configuration Management Data Base/Service Support and peer/hierarchical Network Common Operational Picture systems; queries, receives, and displays additional, more detailed data (as Users drill down from normal displays). Receives and displays security incidents (e.g., Computer Network Attack data) from Security Information Management System. Provides Army Network Common Operational Picture Data/views to the Joint Task Force Global Network Operations' Network Common Operational Picture system.

Organizational Messaging Service Management: In addition to providing the same email service management features noted above (Email underpins Defense Message System-Army), this system enables users to configure and manage unique X.500 Directory variations required to support official Department of Defense Message traffic over Army Radio Frequency and Internet Protocol networks. This includes Defense Message System-Army: 1) Message Transfer Agents; 2) User Agents; 3) Mail List Agents; 4) Directory System Agents; 5) Administrative Directory User Agents; 6) Directory User Agents; 7) Certification Authority Workstations. Provides Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager in accordance with poll/schedule; provides hardware/software inventory, configurations and events/incidents to Configuration Management Data Base/Service Support.

Policy-Based Internet Protocol Network Management: Policy-Based Internet Protocol Network Management creates, manages, authenticates, simulates, stores, and distributes Policy-based Internet Protocol network configuration data files from a central repository, based on pre-defined policies (e.g., Information Operations -3). Enables

users to activate out-of-the-box policies (or customize them), with associated configuration data files, to manage the Internet Protocol transport network (port speeds, switching, routing, etc.) and network security (Access Control List, intrusion detection system/intrusion prevention system signatures, firewall rules, etc.) Policies, and their configuration data files, can be 'stacked' (one imbedded in another). Models Policies' impacts to networks (to authenticate them), then stores and later distributes them (as configuration profiles) when activated. Requests and receives network topology, inventory and configuration data from Internet Protocol Network Management System. Provides events/incidents to Configuration Management Data Base/Service Support; security events to Security Information Management System; configuration profiles to the respective Network Operations systems (e.g., Internet Protocol Network Management System, Firewall Element Manager, Router Element Manager, etc.) for implementation.

Public Key Infrastructure Management: The Public Key Infrastructure Management capability configures and manages Public Key Infrastructure (Certificate Authority servers, Common-Access-Card Cards/Readers, encryption algorithms), services and transactions. This includes configuring and managing all Public Key Infrastructure devices and activities, such as certificate requests and transmittal that interact with the Defense Information Systems Agency external systems. These external authoritative systems include the Defense Information Systems Agency/Global Information Grid Certification Authentication server that issues and validates the certificates that are being used by Network Operations. Public Key Infrastructure Management will include the use of an File Transfer Protocol-based system that will pull from the Defense Information Systems Agency external system entities in order to do requests/gets. Provides certificates and keys to HAIPE managers, upon request. Relies on other Network Operations systems (e.g., Internet Protocol Network Management System and System Management System) for its own configuration, software/operating system updates, and defense.

Remote Access Management: The Remote Access Management Capability configures and manages user access to the network and selected remote Access Points/devices not managed by other Land Warrior Network (LandWarNet) Network Operations Architecture capabilities (RADIUS servers, Terminal Server Access Control System servers, Token bridges/servers; MODEM servers; Virtual Private Network access negotiations; selected Virtual Private Network devices). Provides Security-related Events to Security Information Management System; provides Remote Access Management/Access Points device events/incidents, inventories and configuration data to Configuration Management Database/Service Support; provides Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager.

Router Element Manager: The Router Element Manager configures and manages Open Systems Interconnection Layer-3 (Network) level routers (Army Distribution and Security/ Perimeter Routers) for a specific vendor's routers; includes configuration of routing protocols and policies, Access Control Lists, Networking Address Translation tables, etc.); connected Internet Protocol device reporting, and layer 4

diagnostic/analytic support. Router Element Manager receives and applies router configuration profiles to managed routers; provides router Events/Simple Network Management Protocol Traps, router and attached Internet Protocol device inventories, router configuration data to Internet Protocol Network Management System. Enables Router Element Manager users to access and operate the Internet Protocol Network Management System remotely.

Secure Configuration Remediation (Patch) Management: This system provides the ability to receive vulnerability data from scanners (Internet Protocol Network Vulnerability Scanner and Information Assurance Vulnerability Management Compliance Manager) and use it to configure and apply tailored remediation solutions (patches, configuration changes, or a combination of these) for specific vulnerabilities to specific platforms or platform groups; serves as the authoritative source for computing platform remediation inventory within its sphere of control (e.g., area, theater, unit, etc.) Uses peer-to-peer and hierarchical interactions to form a distributed infrastructure to manage large numbers of computing platforms; does not address proprietary or Government-off-the-Shelf (e.g., Army Battle Command Systems) systems, which have unique software and configurations managed by those vendors/program manager. Provides operational events/incidents, Anti-Virus inventories and configuration to Configuration Management Data Base/Service Support; requests and retrieves updates from authorized external sources.

Secure Sockets Layer Accelerator Element Manager: The Secure Socket Layer Accelerator Element Manager configures and manages Secure Socket Layer Acceleration/ concentration devices. Provides Secure Socket Layer device events/incidents, inventories and configuration data to Configuration Management Data Base/Service Support; provides Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager. It relies on System Management System to configure browsers/Secure Socket Layer software on clients.

Security Information Management System: The Security Information Management System provides a dynamic overview of LandWarNet security, tailored for the viewing user/organization. Filters and aggregates reporting from up to 15 other Network Operations systems, correlates them to known/estimated network attack signatures/pathologies and supports post-attack/trend analyses; connects hierarchically and peer-to-peer to support rapid detection and warning of emerging attacks. Enables users to define and adjust attack signatures/ profiles and to filter out authorized scans/patches; detects information attacks not discernable from individual points/intrusion devices on the network. Security Information Management System provides security-related incidents to Configuration Management Data Base/Service Support for remedial action, and security-based situation data to Network Common Operational Picture for display/monitoring. Supports peer-to-peer and hierarchical connections to support LandWarNet-wide monitoring.

Service Level Manager: Service Level Manager provides LandWarNet Command, Control, Communications, Computers, and Information Management and Information

Technology service management; grants users the capability to plan/define, monitor, analyze and report on the delivery of Command, Control, Communications, Computers, and Information Management and Information Technology services to end users. Provides service modeling, service catalog management, Capacity, Availability, and Performance -based service breach alarms and performance reports. Enables users to pre-plan services needed to support military operations and Continuity of Operations/ Disaster Recovery plans for rapid execution later. Provides agents to simulate traffic to measure end-user performance for key Commercial-off-the-Shelf -based services. Reports tie service performance to impacts/benefits to end-users' operations, training, and business events/missions; supports trend analysis for recurring end-user events. Receives Change Requests (for new/adjusted services) and other Configuration Management Database data from Configuration Management Data Base/Service Support; provides service catalog, service-breach incidents/vents, change requests (to support new/modified services) and Service Level Manager inventory and configuration data to Configuration Management Data Base/Service Support. Requests and processes Capacity, Availability, and Performance Data from Capacity, Availability, and Performance Manager.

Storage Area Network Element Manager: The Storage Area Network Element Manager configures and manages storage area network devices (locally and remotely) from a central manager, with the help of agents/Storage Management Initiative Specification compliant reporting. Enables users to configure access controls to Storage Area Network zones/drives/directories, partition/maintain drives, enact Redundant Arrays of Independent Disks strategies/off-Storage Area Network backups, and provide threshold-based alarms/reporting. Provides operational events/incidents, Storage Area Network inventories and configurations to Configuration Management Data Base/Service Support; sends Storage Area Network devices' Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager.

Systems Management: Systems Management configures and manages general purpose computing assets for the LandWarNet; it's the primary system for general purpose software distribution and installation, patch management, platform inventory, remote platform maintenance, configuration settings control, and user account control. Systems Management is the authoritative source for computing inventory within the LandWarNet. Supports general purpose-host-ready custom applications (e.g., Army Battle Command System software) as a set of files by name, size, date, and/or check-sum. Peer-to-peer and hierarchical links support managing hosts across distributed/military networks. Provides security events/incidents to Security Information Management System; system events/incidents, platform inventory and configurations to Configuration Management Data Base/Service Support; polls for and receives work unit/Trouble Ticket status updates from Configuration Management Database/Service Support; sends platforms' Capacity, Availability, and Performance Data to Capacity, Availability, and Performance Manager. Does not address proprietary or Government-off-the-Shelf systems that are not mounted on general-purpose hosts (those are managed by their vendors/program managers).

Trusted Platform Management: Enables remote/local configuration and management of Trusted Platform Management modules on computing platforms. Allows authorized administrators to take ownership/control of the Trusted Platform Management chip, enabling activation, ownership, and decommissioning of the module, as well as archival of recovery keys.

Virtual Private Network Management: The Virtual Private Network Management system configures and manages Commercial-off-the-Shelf -based Internet Protocol Security/ Secure Socket Layer Virtual Private Network infrastructure and transactions. Provides configuration of Virtual Private Network agents/clients, Virtual Private Network access point/concentrators (access control rules/profiles, Federal Information Processing Standards 140-2 encryption algorithms, packet encapsulation rules/profiles, Virtual Private Network protocols, reporting, etc.) and management of site-to-site and traveling user-to-site Virtual Private Network transactions. Relies on other Network Operations systems to configure Virtual Private Network agents/client systems, control user access, and manage/monitor transactions once connected. Provides Event/Simple Network Management Protocol Trap data and Virtual Private Network inventory (including clients') to Configuration Management Data Base/Service Support. Provides Security-related Events/Simple Network Management Protocol Traps to Security Information Management System and Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager.

Voice Over Internet Protocol Management: Configures and manages Commercial-off-the-Shelf -based Voice Over Internet Protocol infrastructure (call processor/controllers, media/signaling gateways, client/subscribers' Voice Over Internet Protocol devices/ settings).

Wireless Internet Protocol Network Management: The Wireless Internet Protocol Network Management System configures and manages Commercial-off-the-Shelf -based 802.1X Wireless infrastructure connected to Unclassified-but-sensitive Internet Protocol Router Network (NIPRNet). Provides configuration of wireless clients/Network Interface Card, access point devices (access control rules/profiles, Federal Information Processing Standards 140-2 encryption algorithms, device connections per access point, access point signal load balancing rules/profiles, reporting, etc.) Supports connection to Internet Protocol Network Management System or stand-alone (pure wireless local area network) architectures; provides Event/Simple Network Management Protocol Trap data and wireless inventory (including clients') to Internet Protocol Network Management System or Configuration Management Data Base/Service Support. Provides remote control access to Internet Protocol Network Management System; has remote access to that system. Provides Security-related Events/Simple Network Management Protocol Traps to Security Information Management System and Capacity, Availability, and Performance data to Capacity, Availability, and Performance Manager.