BY ORDER OF THE COMMANDER
67TH NETWORK WARFARE WING

67TH NETWORK WARFARE WING
INSTRUCTION 33-1160

1 OCTOBER 2010

Communications and Information

LACKLAND SECURITY HILL ENTERPRISE INFRASTRUCTURE AND COMPUTER SYSTEMS MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

ACCESSIBILITY: Publications and forms are available digitally.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: 690 ISS/SCO

Certified by: 67 NWW/CC
(Colonel Kevin B. Wooton)

Pages: 10

This instruction implements AFPD 33-1, Information Resources Management, AFI 33-112, Information Technology Hardware Asset Management, AFI 33-114, Software Management, and AFI 33-115V1, Network Operations (NetOps). It provides standard processes and procedures and sets forth responsibilities for effective management and control of Lackland Security Hill Enterprise (LSHE) networks, systems, and architectures. It also provides guidance to ensure standardized, interoperable, and secure network systems capable of effective support to the Air Force Intelligence, Surveillance & Reconnaissance Agency (AF ISR Agency) information operations mission. LSHE computer networks operate at different security classification levels and are critical resources for field units in effectively accomplishing their objectives. This instruction provides management guidance for these networks and associated hardware (HW) and software (SW) systems. It applies to domain users supported on the LSHE networks within AF ISR Agency directorates and major staff offices, the 24th Air Force (24 AF), the 67th Network Warfare Wing (67 NWW), the 688th Information Operations Wing (688 IOW), Cryptologic Systems Group (CPSG) and other units not covered under a separate Service Level Agreement (SLA). Other collocated AF ISR Agency and non-AF ISR Agency organizations, such as the Joint Information Operations Warfare Center (JIOWC) which may operate one or more separate networks interfacing with the AF ISR Agency networks and must negotiate a SLA with the 690th Network Support Group (690 NSG) (see paragraph 6.) Ensure all records created as a result of processes in this publication are maintained in accordance with AFMAN 33-363, Management of Records, and AFISRA SUP_1 to AFMAN 33-363, and disposed of in accordance with the Air Force Records Information Management System (AFRIMS) Records Disposition Schedule located at **https://afrims.amc.af.mil/rds_series.cfm**. Submit recommendations for changes to this instruction on AF Form 673, Air Force

Recommendation for Change of Publication, through channels to 690 NSG/MS, 102 Hall St., Ste 146, San Antonio, TX 78243.

1. Scope. The LSHE is comprised of the network infrastructure, servers, workstations, and software managed by 690 NSG supporting AF ISR Agency, the 24 AF, the 67 NWW, 688 IOW, and tenants within the Security Hill Complex, Lackland AFB, TX. This does not include mission systems that are behind "firewalls" and are managed by these respective organizations. The JIOWC is a collocated unit that manages their own network infrastructure but have a direct interface to the LSHE. These organizations have specific roles and responsibilities as members of the LSHE. There are three distinct local area networks (LANs) that form the backbone of the LSHE and provide worldwide connectivity between the Department of Defense (DoD) Intelligence Community and other authorized activities. There are also four minor networks managed and maintained within the LSHE to support specific functions or missions.

1.1. Joint Worldwide Intelligence Communications System (JWICS). The JWICS LAN is a Top Secret/Special Compartmented Information (TS/SCI) United States only network controlled by Defense Intelligence Agency (DIA) to support collaboration of intel data within the DoD. DIA has delegated management of the Air Force service component to the AF ISR Agency.

1.2. National Security Agency Network (NSANET). The NSANET is a TS/SCI 5-eyes network controlled by National Security Agency (NSA) to support collaboration of intel data between the US and allies. NSA has delegated the management of the network to Control Security Service Texas (CSSTEXAS).

1.3. Secret Internet Protocol Routing Network (SIPRNET). The SIPRNET network is part of the AFNetOps communication structure managed by 24 AF. Core SIPRNET services are managed by the Integrated Network Operations Security Center with the Lackland AFB Network Control Center functions being performed by the 690th Intelligence Support Squadron (690 ISS).

1.4. Minor networks. LSHE includes access to management of several minor networks which include the Open Source Information System, Roadrunner, StoneGhost, and the Central Intelligence Agency network.

1.5. The Unclassified LAN provides access to the non-classified Internet Protocol Routing Network (NIPRNet) controlled by the 802nd Communication Squadron (802 CS).

2. Roles and Responsibilities.

2.1. Communications and Information Systems Officer (CSO). The Commander of the690 NSG is designated as the LSHE CSO. The LSHE CSO will have the same duties and responsibilities as a base CSO for the three classified networks and will perform these duties and responsibilities in concert with the Lackland base CSO for the unclassified network as outlined in AFI 33-112, Information Technology Hardware Asset Management, AFI 33-115, V1, Network Operations (NETOPS), and the C4 systems planner duties outlined in AFI 33-104, Base-Level Planning and Implementation. In addition, the LSHE CSO will:

2.1.1. Develop and maintain a documented requirements process for the LSHE.

2.1.2. Manage day-to-day operations and maintenance of the LSHE and provide operations and maintenance services that are outside the responsibilities of the Client Support Technician (CST) for all hardware and software standard configurations throughout the LSHE.

2.1.3. Plan and implement AF ISR Agency target architectures.

2.1.4. Develop and implement an enterprise configuration management plan for LSHE.

2.1.5. Appoint a LSHE Equipment Control Officer (ECO) for DRA 5100.

2.1.6. Appoint a LSHE Unit Software License Manager (USLM).

2.1.7. Appoint an LSHE Communications and Information Systems Installation Records (CSIR) Manager. The LSHE CSIR Manager performs the duties and responsibilities of a base CSIR Manager for AF ISR Agency facilities and controlled areas.

2.1.8. Develop and implement a program to train and certify CSTs.

2.1.9. As the Technical Solution (TS) authority for LSHE, provide approved TS for all Communications and Information requirements on the LSHE.

2.1.10. Develop and maintain a Standard Level of Service (SLS) agreement for all LSHE supported organizations.

2.1.11. Develop and maintain policies to obtain and remove user accounts.

2.2. Collocated and Support Units will:

2.2.1. Follow the 690 NSG requirements management process for the LSHE.

2.2.2. Coordinate all proposed changes to the LSHE or its interfaces with the CSO through the LSHE AF Form 3215 (Information Technology/National Security System Requirements Document) or automated process. Do NOT send requests (AF 3215 or automated system) to 690 NSG that are not fully funded.

2.2.3. Negotiate an appropriate support agreement, Memorandum of Agreement (MOA), or SLA, if necessary, for the required level of support to be provided above the SLS.

2.2.4. Organizational Commanders will appoint Equipment Custodian (EC) for their organizations.

2.2.5. Each organization appoints a sufficient number of CSTs to ensure adequate support to their customer base. The CST is the initial level of response to problems and the customer's first source for computer help. CSTs must achieve local certification on network operating systems before they perform CST duties. Certification ensures the CST possess the necessary skills and knowledge to perform effectively.

3. User Accounts.

3.1. General User Accounts. General user accounts are issued to personnel who require access to the LSHE on a routine basis for official duties. A USERID and password with limited privileges is given to a specific person so that he/she may be able to access LSHE resources (JDCSISSS 6.3.1).

3.1.1. Computer users must complete initial DoD Information Assurance Awareness training prior to obtaining access to the network. The standard procedures for obtaining a new account are as follows:

3.1.2. CST will assist users, requesting access, by filling out Part 1 of the Access Request and Verification (67 NWW IMT 10) for SIPRNET/JWICS account and/or NSA Form G6521 for NSANET accounts.

3.1.3. User will meet with their respective supervisor who will then complete Part 2 of 67 NWW IMT 10 and/or NSA Form G6521.

3.1.4. If the user is requesting a SIPRNET or JWICS account:

3.1.4.1. The CST will assist the new user with completing the required network licensing training and annotate the results in Part 1, Item 15, of the 67 NWW IMT 10. The appropriate Security Office will complete Part 3 of the 67 NWW IMT 10 after performing eligibility verification. If the new user is eligible, the 67 NWW IMT 10 will then be forwarded to the 690 ISS/SCOS Help Desk for account creation and issue of a USERID/password.

3.1.4.2. When users pick up their USERID and password they will then sign in block 42 of Part 5, of 67 NWW IMT 10 acknowledging responsibility for USERID and password. Signature of a user agreement form may also be required.

3.1.5. If the user is requesting an NSA account:

3.1.5.1. The CST will assist the new user with completing Part 2 of the NSA Form G6521. The NSA Form G6521 will then be forwarded to the AF ISR Agency/SOP office for eligibility verification. Once the user has been verified eligible, the form is then forwarded to the Help Desk for account creation and completion of Part 4. Signature of a user agreement form may also be required.

3.1.5.2. When users pick up their USERID and password they will then sign in block 42 of Part 5, of 67 NWW IMT 10 acknowledging responsibility for USERID and password. Signature of a user agreement form may also be required.

3.1.6. Account modifications or deletions, as well as Public Key Infrastructure (PKI) certificates, will be requested using the 67 NWW IMT 10 or NSA Form G6521 with proper annotations. This documentation will provide the pertinent user information, verify required training, and identify the required level of service.

3.1.7. Foreign national users must clearly identify their nationality on the 67 NWW IMT 10, item 11b.

3.1.8. User accounts must be suspended if going TDY for 60 days or more or any other extended period of absence. The responsible Information Assurance Officer (IAO) will ensure that all user accounts are annotated as such.

3.2. Privileged User Accounts (Administrator). Privileged user accounts are given to personnel who have the need to perform functions on the network that require privileges beyond the scope of a general user account. Any use of these privileges must be for official duties only. Additionally, this account is issued only after the person has received system administrator training or CST training.

3.2.1. The 690 ISS Enterprise Operation Center (EOC) is responsible for maintaining the LSHE throughout day-to-day operations, ensuring that the system operates within established accreditation criteria and keeping the system in an operational mode for general users.

3.2.2. Domain administrator rights will be minimized only to qualified system administrators. The 690 ISS/SCXN Configuration Management section must have a request in writing in order to approve all domain administrator accounts. This is to ensure only qualified system administrators are given access to critical network system resources.

3.2.3. No user will have access credentials that allow him/her to logon to a system without authenticating with a network authentication provider (i.e., Domain Controller, Network Information Service Controller). The 690 ISS/SCXN Configuration Management section must approve any variance from this.

3.2.4. The local administrators group on all systems will include the following groups: domain administrators, 690 ISS Help Desk, Server Management System client account, and respective organizational CST groups. These are the only types of groups to be added into the local administrators group on a workstation.

3.2.5. Any user requesting greater than normal privileges on a specific system must have those privileges approved by the IAO and the Information Assurance Manager (IAM). Any change to the local system configuration or security settings is not authorized.

4. Invalid Accounts.

4.1. Guest Accounts. Guest accounts are defined as temporary, general use accounts that allow extremely limited access to the network without requiring a uniquely identified USERID (i.e., guest anonymous, etc.) This type of account is not allowed on the LSHE networks and is disabled by default.

4.2. Group Accounts. Group accounts are strictly prohibited on the LSHE networks. Group accounts are accounts that share a logon account with a single USERID and password. Group accounts cannot be traced back to a specific person during an audit review.

4.3. Inactive Accounts. An inactive account is any account that has not been used in the past 30 days.

4.3.1. The system administrators/client support technicians (SA/CST) will be responsible for notifying the 690 ISS Help Desk anytime a user's account will be inactive for more than 30 days. If the individual will be accessing their account using Outlook Web Access, do not provide any notification for that account.

4.3.2. All notifications must be submitted in writing (67 NWW IMT10, NSA Form G6521 or memo for record). If the return date is changed, the SA/CST needs to inform the Help Desk so the account can be modified to reflect the new date. Upon return, the SA/CST must notify the Help Desk in order to ensure that the account is reinstated.

4.3.3. If an account is found to be inactive and no information has been received to indicate an individual is TDY, leave, etc., the account will be disabled, and the e-mail account will be placed on a 30-day hold. If no notice is received within those 30 days (a total of 60 days), the exchange account will be permanently deleted. It is the

responsibility of the SA/CST to keep the Help Desk informed on user absences, and it is user's responsibility to keep the SA/CST informed.

5. Support for Non-Standard Implementations.

5.1. Validated requirements that can be satisfied only by non-standard implementations will be addressed on a case-by-case basis. To ensure life cycle support is available, the CSO will not approve any implementation until adequate logistics support is addressed and funded for the LSHE.

5.2. Proposed solutions for the LSHE that do not comply with current standards will be elevated to the Chief Information Officer Working Group (see AFISRASUP 1 to AFI 16-501, Control and Documentation of Air Force Programs) for review and disposition.

6. Service Level Agreement (SLA).

6.1. Supported organizations with requirements exceeding the SLS must negotiate a SLA for support of that particular requirement. The SLA defines the relationship and the services the CSO will provide and the requesting organization's responsibilities, including funding, when necessary.

6.2. For supported organizations with requirements exceeding the SLS, a signed SLA must be in effect before establishing an interface between the LSHE and networks maintained by other organizations in order to maintain network security and ensure effective configuration management.

7. Computer Systems Acquisition.

7.1. All requests for Information Technology (IT) acquisition, both HW and SW, impacting the LSHE or its interfaces, excluding mission systems that are behind "firewalls" and are managed by other organizations, will be submitted on a validated AF Form 3215 or automated system to 690 ISS/SCXP. The Validation Requirement Officer (VRO), unit commanders or their designated representative must sign the AF Form 3215 to validate the requirement.

7.2. A TS will be developed to meet the validated requirements.

7.3. IT items will be selected from the approved/recommended list of software and hardware in the NSA Enterprise Solution (NES), the Air Force Evaluated/Approved Product List (E/APL) or the 802 CS policy, in that order.

7.4. Purchases of IT items will follow the specifications in the CSO approved TS and will be made through appropriate Air Force procurement channels.

7.5. Equipment that does not meet the enterprise configuration management criteria will not be connected to the LSHE.

8. Transfers or Removal of Computer Hardware or Software.

8.1. The LSHE USLM coordinates with the EOC to ensure all software is removed or transferred and accounts for all site software licenses.

8.2. The responsible EC coordinates with the respective unit IAM and the Security Office on the transfer or removal of communications and information equipment connected to any LSHE network. The appropriate security accreditation packages are reviewed and updated

by the IAM and coordinated through the information assurance office. Further guidance can be found in the JDCSISSS, Joint DoDIIS/Cryptologic SCI Information Systems Security Standards.

8.3. The EC coordinates with the ECO to ensure proper turn-in and records management for each equipment item.

KEVIN B. WOOTON, Colonel, USAF
Commander

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFPD 33-1, *Information Resources Management*

AFI 33-104, *Base-Level Planning and Implementation*

AFI 33-108, *Compatibility, Interoperability, and Integration of C4 Systems*

AFI 33-112, *Information Technology Hardware Asset Management*

AFI 33-114, *Software Management*

AFI 33-115, *Network Operations (NETOPS)*

AFI 16-501, *AFISRA SUP1 Control and Documentation of Air Force Programs*

690 NSG LSH Communications and Information Systems Requirement Document Process Handbook

JDCSISSS Joint DoDIIS/ Cryptologic SCI Information Systems Security Standards

AF—Air Force

AFI—Air Force Instruction

AFNetOps—Air Force Network Operations

AF ISR Agency—Air Force Intelligence, Surveillance & Reconnaissance Agency

CST— Client Support Technician

CSIR—Communications and Information Installation Records

CSO—Communications and Information Systems Officer

DIA—Defense Intelligence Agency

DoD—Department of Defense

EC—Equipment Custodian

ECO—Equipment Control Officer

EOC—Enterprise Operations Center

HW—Hardware

IAM—Information Assurance Manager

IAO—Information Assurance Officer

IOW—Information Operation Wing

IT—Information Technology

JIOWC—Joint Information Operations Warfare Center

JWICS—Joint Worldwide Intelligence Communications System

LAN—Local Area Network

LSHE—Lackland Security Hill Enterprise

MOA—Memorandum of Agreement

NES—NSA Enterprise Solution

NETOPS—Network Operations

NIPRNET—Nonclassified Internet Protocol Routing Network

NSA—National Security Agency

NSANET—National Security Agency Network

NSG—Network Support Group

NWW—Network Warfare Wing

PKI—Public Key Infrastructure

SA—System Administrator

SIPRNET—Secret Internet Protocol Routing Network

SLA—Service Level Agreement

SLS—Standard Level of Service

SW—Software

TS—Technical Solution

TS/SCI—Top Secret/Special Compartmented Information

USLM—Unit Software License Manager

VRO—Validation Requirement Officer

WG—Working Group

Terms

Configuration Management—A discipline applying technical and administrative direction and surveillance to:

(a) Identify and document a baseline;

(b) Control changes to the baseline;

(c) Provide the status of the implementation process; and

(d) Perform audits

Information System—Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data and includes computer software, firmware, and hardware.

Local Area Network (LAN)—A LAN has the capability to provide local interoperability between physically separated computer systems.

Network—A combination of information transfer resources devoted to the interconnection of two or more distinct devices, systems, or gateways.

Non-Standard Implementation— Implementation of HW or SW on the NSANET that is not listed on the NES or implementation of HW or SW on JWICS, SIPRNET or NIPRNET that is not listed on the E/APL.

Operation—Supports the user with day-to-day ability to access and process authorized information transferred or stored on the LANs and networks.

Validation Requirement Officer—The person given responsibility for overall management of organizational IT systems. In addition to the organizational head (i.e., director, commander, etc.), the person that approves organizational IT requirements, signs the AF Form 3215 as the organizational representative, and manages and/or advises the organizational head on SLA issues and recertification. The VRO is responsible for ensuring that all copyrighted software used in the organization is properly licensed in accordance with AFI 33-114. The VRO (or a designee such as the system administrator or client support technician) must maintain inventory of all nonstandard software (whether installed or not), must identify nonstandard software installed on each computer, and must store valid proof of license in a secure location. Software inventories will be provided to the USLM in the USLM supplied format. The VRO must ensure all personnel are trained on software license management policy. The VRO must perform an annual audit of the nonstandard software inventory.

Resources—Include but are not limited to funding, equipment, personnel, time or space.

Unit Software License Manager (USLM)—The USLM develops site policies, procedures, and training material to oversee and track site purchased licenses, coordinates and periodically audits CST activities, provides software inventory format in accordance with AFI 33-114, and monitors the site-wide software license annual inventory.

Standard configuration for HW and SW—For SIPRNET and NIPRNET HW and SW must be listed on E/APL, approved by the Information Technology Commodity Council and purchased through AFWay provides the standard configuration. NSANET and JWICS requires SW reloads by the CST during initial installation.

Standard level of service—The service that is provided to customers using standard configurations for HW and SW.