PEO C3T

PROGRAM EXECUTIVE OFFICE COMMAND CONTROL COMMUNICATIONS-TACTICAL

PROJECT MANAGEMENT OFFICE NETWORK ENABLERS

# Project Lead Network Enablers (PL Net E)
# Security Classification Guide (SCG)

**Distribution Statement D:** Distribution authorized to Department of Defense (DOD) and United States (US) DOD contractors only, by specific authority of Army Regulation (AR) 380-5, for administrative and operational use. Date of determination is approval date of this document. Other requests for this document shall be referred to the Office of the Project Lead, Network Enablers (PL Net E, SFAE-CCC-NE), 6560 Surveillance Loop, F5-118, Aberdeen Proving Ground (APG), MD 21005.

# PL Net E SCG

**Issued By:** PL Net E
SFAE-CCC-NE
6560 Surveillance Loop, F5-101
APG, MD 21005

**Approved By:**

MG DAVID G. BASSETT
Program Executive Officer
Program Executive Office Command, Control, Communications–Tactical (PEO C3T)

**Date:** 24 may 2018

**Program Number:** None

**Supersession(s):** PL Net E SCG, dated 22 August 2015

**Action Officer(s):** Stanley M. Niemiec
PL Net E
SFAE-CCC-NE
6560 Surveillance Loop, F5-101
Aberdeen Proving Ground, MD 21005
(443) 395-2318

**Distribution Statement D:** Distribution authorized to Department of Defense (DOD) and United States (US) DOD contractors only, by specific authority of Army Regulation (AR) 380-5, for administrative and operational use. Date of determination is approval date of this document. Other requests for this document shall be referred to the Office of the Project Lead, Network Enablers (PL Net E, SFAE-CCC-NE), 6560 Surveillance Loop, F5-118, Aberdeen Proving Ground (APG), MD 21005.

# TABLE OF CONTENTS

## SECTION 1 – GENERAL INFORMATION

**1.1 Purpose.** To provide instructions and guidance on the security classification of information and material pertaining to the PL Net E products. The products include Tactical Network Initialization and Configuration (TNIC), Network Products Development (NPD), Automated Communications Engineering Software (ACES) Workstation, Simple Key Loader (SKL), and other products managed by PL Net E or subordinate product offices. It provides classification guiadance PL Net E, product offices part of PL Net E, support divisions (e.g.; Readiness Management Division,) and contractors.

**1.2 Authority.** This SCG is issued under the authority of AR 380-5, 29 Sep 00; E.O. 13526, "Classified National Security Information," 29 Dec 09; and DOD Manual 5200.01, "DOD Information Security Program: Overview, Classification, and Declassification" Volumes 1-4, 24 Feb 12. It constitutes authority and may be cited as the basis for classification, regrading or declassification of information concerning PL Net E products and information. Unless otherwise noted, the authority of the approving official on the title page classifies information or material identified as classified in this SCG. Information marked as classified in accordance with (IAW) the guidance provided in this SCG must be additionally marked with the following statement:

Derived from: PL Net E SCG
Declassify on: (Date or event specifically mandated by this guide)

**1.3 Application**. Per AR 380-5, this SCG will be reviewed and updated for each subsequent version every five years, as a minimum, or sooner if circumstances dictate. If the Office of Primary Responsibility (OPR), PL Net E, recognizes an administrative or guidance change that must be made to the SCG, the required change will be made immediately and reported in writing by the OPR to the Program Executive Officer Command Control Communications – Tactical (PEO C3T) Security Manager, ATTN: SFAE-CCC-CSO, 6590 Reconnaissance St, APG, MD 21005 for review, processing and dissemination. If there is a conflict between this guide and the NSA/CSS KMI Classification Guide 3-4, 28 Jan 15, the NSA KMI CG 3-4 will take precedence.

**1.4 Questions and Recommendation**. Questions concerning the content and interpretation of this SCG will be directed to the OPR. If the security classification imposed by this SCG is considered impractical, documented and justified recommendations will be made through appropriate channels to the OPR. If current conditions, progress made in this effort, scientific or technological developments, advances in the state-of-the-art, or other factors indicate a need for changes, similar recommendations should be made. Pending a final decision, the information involved will be protected at either the currently specified level or the recommended level, whichever is higher. All users of this SCG are encouraged to assist in improving its currency and adequacy. Any over-classification or incorrect classification will be brought to the attention of the OPR, who will report these changes in writing to the PEO C3T Security Manager, ATTN: SFAE-CCC-CSO, 6590 Reconnaissance St, APG, MD 21005-1848.

**1.5 Public Release**. The fact that this SCG shows certain details of information to be unclassified does not authorize automatic public release. Classified information shall not be declassified automatically as a aresult of any unauthorized disclosure or release of identical or similar information. Proposed public releases of unclassified information regarding PL Net E products must be processed through appropriate channels for approval for publication. Within the Department of the Army, the procedures specified in AR 360-1, "The Army Public Affairs Program" will be followed. Defense contractors will comply with DoD 5220.22-M (National Industrial Security Program Operating Manual – NISPOM) and other contractual requirements. All information pertaining to PL Net E products that is proposed for public release must undergo a formal security classification and policy review process prior to official public release. All information requested for public release concerning PL Net E products will be forwarded to the PEO C3T Public Communications Directorate, ATTN: SFAE-CCC-CSO, 6590 Reconnaissance St, APG, MD 21005, in accordance with (IAW) AR 360-1, paragraph 5-3, proir to public release.

**1.6 Definitions and Acronyms.**

**1.6.1 Definitions.**

| | |
|---|---|
| **LDIF** | LDAP (Lightweight Data Application Protocol) Directory Interchange Format – Allocation of ABCS equipment and assignment of IP addresses built through the AIM tools |
| **Level 1 Engineering Designs:** | Information that identifies the entire defense materiel item, a program element, project or subprogram, for example, an electronic system. An "electronic system" might be a command and control system, a radar system, a communications system, a management information system, a sensor system, navigation or guidance system, or electronic warfare system. |
| **Level 2 Engineering Designs:** | Information that identifies the major elements subordinate to the Level 1 major elements, for example, an air vehicle of a missile or aircraft system, or the complete round of an ordnance system. These major elements are prime mission products, which include all hardware and software elements. Level 2 elements also include aggregations of system level services (like system test and evaluation, or systems engineering and program management), and data. |
| **Level 3 Engineering Designs:** | Information that identifies elements subordinate to Level 2 major elements, including hardware and software and services. For example, the radar data processor of the fire control radar or, the Developmental Test and Evaluation (DT&E) subordinate element of System Test and evaluation, or technical publications element of Technical Data. Lower levels follow the same process. |

### 1.6.2 Acronyms.

| | | |
|---|---|---|
| ACA: Army Certification Authority | ACES: Automated Communications Engineering Software | ACL: Access Control List |
| AIC: Army Interoperability Certification | AIM: Automated Initializaton Manager | AKMI: Army Key Management Infrastructure |
| AKMS: Army Key Management System | AMDWS: Air and Missile Defense Workstation | APG: Aberdeen Proving Ground |
| AR: Army Regulation | ATO: Authority To Operate | ATS: Automated Tactical Systems |
| CCB Configuration Control Board | CM: Configuration Management | COMSEC: Communications Security |
| COTS: Commercial Off The Shelf | DoD: Department of Defense | DTP: Detailed Technical Procedures |
| E.O.: Executive Order | EKMS: Elecetronic Key Management System | FOIA: Freedom of Information Act |
| FBCB2: Force XXI Battle Command Brigade and Below | FMS: Foreign Military Sales | IAVA: Information Assurance Vulnerability Alert |
| FOUO: For Official Use Only | GOTS: Government Off The Shelf | IP: Internet Protocol |
| IAVB: Informatin Assurance Vulnerablity Bulletin | IO: Information Operations | KMI: Key Management Infrastructure |
| LCMS: Local Communications Security (COMSEC) Management Software | JBC-P: Joint Battle Command – Platform | LDIF: (Lightweight Data Application Protocol) Directory Interchange Format |
| MGC: Management Client, one type of KMI client node | LDAP: Lightweight Data Application Protocol | MOU: Memorandum of Understanding |
| NDP-1: National Disclosure Policy - 1 | MOA: Memorandum of Agreement | NSA: National Security Agency |
| OPR: Office of Primary Responsibility | NPD: Network Products Development | PI: Program Integrator |
| POM: Program Objective Memorandum | PL Net E: Project Lead Network Enablers | SA: System Architecture |
| SFA: Self Funded Application | RMF: Risk Management Framework | SKL: Simple Key Loader |
| SOI: Singal Operating Instructions | SIP: System Identification Profile | TNIC: Tactical Network Initialization and Configuration |
| TRRs: Tactical Radio Reports | SOP: Standarde Operating Procedures | URL: Uniform Resource Locator |
| URN: Unit Reference Number | UAT: User Acceptance Testing | USAFMSA: United States Army Force Management Support Agency |
| UTO: Unit Task Organization | U.S.: United States | |

**1.7 Foreign Government Information**. Not-Applicable at this time. If foreign government information is received to become incorporated within any PL Net E product, this SCG will be revised.

**1.8 Foreign Disclosure**. Any disclosure to foreign officials of information classified by this SCG shall be in accordance with the procedures set forth in AR 380-10 and National Disclosure Policy – 1 (NDP-1). If a country with which the Department of Defense (DoD) has entered into a reciprocal procurement memorandum of understanding or offset arrangement expresses an interest in this effort, a foreign disclosure review will be conducted prior to issuance of a solicitation.

**1.9 Foreign Military Sales**. The ACES workstation and the SKL are currently approved for FMS. Any FMS-related issues shall be referred to and coordinated with PL Net E. The LCMS and KMI workstations are National Security Agency (NSA) products and FMS must be coordinated with that agency for those items.

**1.10 Systems Descriptions**.

**1.10.1 TNIC NPD.** The TNIC NPD system of systems is a collection of network initialization products, development tools, and CM tools, including the Quality Assurance/Quality Control Tool, Configuration Generation Builder, and CM Database, which provide a means to produce network initialization data products for the US Army. The TNIC applications use a phased approach to build US Army network initialization data products. The Configuration Generation Builder is used to generate a set of baseline network configurations for the US Army tactical unit system architecture, as well as configurations for testing, training, and unit specific mission sets. This set of configurations is stored in a centralized online database hosted via Military Techical (MilTech) Solutions and distributed securely via the TNIC Configuration Management (CM) process. The configurations are then processed by the Quality Assurance/Quality Control Tool for formal review and distributed to appropriate parties via the TNIC NPD CM process. Formal documentation, including network diagrams, interconnectivity diagrams, and IP allocation spreadsheets are also produced and distributed. TNIC NPD Development products are ultimately used by US Army units to initialize their Tactical Internet.

**1.10.2 AIM.** AIM is a stand-alone system that provides a means to produce US Army Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance initialization data products required to enable end-to-end network centric connectivity, interoperability, and visibility across the US Army Tactical Internet. See Section 4 of this SCG for data elements relating to classification of data products.

**1.10.3 AKMS.** The AKMS is comprised of the ACES workstation, the NSA certified cryptographic key fill device, the SKL, and the LCMS workstation. AKMS provides the framework for interface to the NSA developed Electronic Key Management System (EKMS), allowing joint service interoperablity between the individual service automated KMS. AKMS integrated all functions of theater/tactical cryptographic key distribution and management into a single system of systems. AKMS provided for automation of the then manual cryptonet planning and cryptonet management processes, including the generation and distribution of Signal Operating Instructions (SOI) data and Electronic Protection (EP) fill data to support combat net radio operations.

**1.10.4 AKMI.** The Army Key Management Infrastructure (AKMI) is the next generation system replacing the AKMS. It is comprised of NSA KMI client nodes, of which one type of node is the Management Client (MGC); the ACES workstation, and the SKL. The Army will field the NSA developed KMI client nodes to replace the LCMS workstations.

**1.10.5 Team C4ISR Aquistion Network (TCAN).** The Team C4ISR Acquisition Network provides the US Army with collaborative and informational web sites. These websites are critical to both CONUS and OCONUS operations.

**1.10.6 milSuite.** A suite of tools to provide peraonalized ans social media capabilities to support a virtual workforce. Allos the workforce to connect with people and knowledge instantly for collaboration and secure sharing of information behind the firewall. Tools within the suite include milWiki, milWire, milBook, and milTube and other additonal services.

**1.11 References.**

**1.11.1 Required Reference Publications.**

(a) Executive Order (E.O.) 13526, Classified National Security Information, 29 Dec 2009
(b) AR 380-5, Department of Army Information Security Program, 29 Sep 2000
(c) DOD Manual 5200.01, DOD Information Security Program, dated 24 Feb 2012, Incorporating Change 2, 19 Mar 2013
(d) NSA/CSS Classification Guide for KMI 3-4, 28 Jan 2015

**1.11.2 Other Related Publications.**

(a) Army Automated Tactical Systems SCG, Sep 2014
(b) AR 25-55, " The Department of the Army Freedom of Information Act Program," 01 Nov 1997
(c) C-E LCMC Regulation 380-3, SCG Procedures, 31 Jul 2008
(d) DOD Directive 8500.01, "Cybersecurity," 14 Mar 2014
(e) DOD Directive 5230.9, "Clearance of DOD Information for Public Release," 22 Aug 2008, as ammended
(f) DOD Instruction O-3600.02, "Information Operations (IO) Security Classification Guidance (U)," 28 Nov 2005

(g) DOD Manual 5200.45, "Instructions for Developing SCG," 2 Apr 13
(h) DOD Instruction 8510.01, "Risk Management Framework (RMF) for DOD Information Technology (IT)," 12 Mar 2014
(i) AR 25-2, "Information Assurance," 23 Mar 2009
(j) AR 380-10, "Foreign Disclosure and Contacts with Foreign Representatives," 14 August 2015

**1.12 Reasons to Classify.** The reasons for classifying information in this SCG are IAW Part I, Section 1-4, E.O. 13526. Specific to this SCG are the following reasons:

1-4 (a): Military Plans, weapons systems, or operations
1-4 (b): Foreign government information
1-4 (c): Intelligence activities (including covert actions), intelligence sources or methods, or cryptology
1-4 (d): Foreign relations or foreign activities of the United States, including confidential sources
1-4 (e): Scientific, technological, or economic matters relating to national security, which includes defense against transnational terrorism
1-4 (f): United States Government programs for the safeguarding of nuclear materials or facilities
1-4 (g): Vulnerabilities or capabilities of systems, installations, infrastructures, projects, or protection services relating to the National Security, which includes defense against transnational terrorism
1-4 (h): The developmet, production, or use of weapons of mass destruction

**1.13 For Official Use Only (FOUO) Caveat.** FOUO is not a security classification. Information that has not been given a security classification pursuant to the criteria in this guide, but which may be withheld from the public for one or more of the reasons cited in the Freedom of Information Act (FOIA) exemptions, AR 25-55, Army Freedom of Information Act Program, shall be designated FOUO. Information so designated in this guide that warrants FOUO markings will be handled and protected IAW the above-cited regulation.

## SECTION 2 – OVERALL EFFORT

Note: The following data elements tables apply to PL Net E products unless otherwise specified

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **2.1 General Details** | | | | |
| 2.1.1 Program Name | U | | | |
| 2.1.2 Description | U | | | |
| 2.1.3 Software Version | U | | | |
| 2.1.4 Nomenclature | U | | | |
| 2.1.5 Army Portfolio Management System (APMS) Number | U | | | |
| 2.1.6 Program Mission | U | | | |
| **2.2 Contractor Relationships (the association of specific vendors)** | U | | | |
| **2.3 Program Resources** | | | | |
| 2.3.1 Funding level (budget information which includes specific dollar amounts allocated to a specific project or program) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 2.3.2 Overall budget by year, category, and system; (for example POM submission) | | | | Mark as FOUO.Specific budget information includes information such as specific dollar amounts allocated to a specific project or program. |
| 2.3.2.1 Pre-POM Submission | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 2.3.2.2 After-POM Submission | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 2.3.3 Identification of particular installation, facility or range associated | U | | | General identification of Program Management Office/PEO and prime contractor is public releaseable. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 2.3.4 Information about related facilities that reveal specific production details (for example capacity, volume, delivery schedules, etc.) to a particular client | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **2.4 End Item** | | | | |
| 2.4.1 Hardware and Firmware | U | | | Classified Cryptographic key material will be stored IAW the level of classification. Unclassified cryptographic key material will be stored IAW approved controlled crytographic item (CCI) procedures for handling of CCI items. IAW reference 1.11.1.d, hardware and software maybe classified under the authority of the NSA. |
| 2.4.2 Military Application | U | | | |
| 2.4.3 Internal View | See Remarks | | | Internal views of NSA certified devices (for example SKL) may be classified under the authority of the NSA. See applicable NSA documentation to get clasification guidance. |
| 2.4.4 External View | U | | | |
| 2.4.5 Software | | | | |
| 2.4.5.1 COTS (for example Windows Operating System software information such as make, model, version name or number included with a client node) | U | | | Mark as FOUO. FOIA Exemption 4 applies. Derived from NSA KMI SCG. |
| 2.4.5.2 GOTS (for example ACES or SKL software information such as make, model, version name or number included with a client node) | U | | | Mark as FOUO. FOIA Exemption 4 applies. Derived from NSA KMI SCG. |

## SECTION 3 – PERFORMANCE AND CAPABILITIES

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **3.1 General information** regarding the capabilities of PL Net E systems, specific system, subsystems, or components | U | | | Level 1 engineering design specifications only. |
| **3.2 Specific details** (regarding the performance of either PL Net E specific system, subsystems, or components | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

## SECTION 4 – SPECIFICATIONS

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **4.1 NPD - Quality Assurance/Quality Control Tool** | | | | |
| 4.1.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.1.2 Detailed design specifications, including specific configuration requirements reviewed during the quality analysis review | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.2 NPD - Configuration Generation Builder** | | | | |
| 4.2.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.2.2 Detailed design specifications regarding the configuration tool utilized by TNIC NPD to include detailed script or configuration output information | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.3 NPD - CM Database** | | | | |
| 4.3.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.3.2 Detailed design specifications regarding the TNIC NPD CM Database, to include detailed hardware baseline, software baseline or configuration process | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.4 AIM - Quality Assurance/Quality Control Tool** | | | | |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 4.4.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.4.2 Detailed design specifications, including specific configuration requirements reviewed during the quality analysis review | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.5 AIM - Configuration Generation Builder** | | | | |
| 4.5.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.5.2 Detailed design specifications regarding the configuration tool utilized by TNIC NPD to include detailed script or configuration output information | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.6 AIM - CM Database** | | | | |
| 4.6.1 General information regarding design specifications/physical characteristics | U | | | |
| 4.6.2 Detailed design specifications regarding the AIM CM Database, to include detailed hardware baseline, software baseline or configuration process | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **4.7 COMSEC Key Specifications** | | | | |
| 4.7.1 Transmission Security Key | U | | | |
| 4.7.2 COMSEC Key for unclassified system | U | | | |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 4.7.3 COMSEC Key for classified system | See Remarks | | | COMSEC key specifications for NSA certified systems are classified, if appropriate, under the authority of the NSA. NSA classification guidance must be consulted. |
| 4.8 MilTech Systems | | | | |
| 4.8.1 Team C4ISR Acquisiton Network (TCAN) | U | | | The system holds a varity of inforamtion from different members of the DoD community. This means the data could potentially be corrilated and change the classification from the standard Unclassified to a higher level. The system is approved to hold up to U//FOUO information. In addtion, multiple applications hosted on the system are authorized to house Personally Idenifiable Inforamtion (PII). This adds another layer of security to the overall system. |
| 4.8.2 milSuite | U | | | The system holds a varity of inforamtion from different members of the DoD community. This means the data could potentially be corrilated and change the classification from the standard Unclassified to a higher level. The system is approved to hold up to U//FOUO information. |

## SECTION 5 –VULNERABILITIES AND WEAKNESSES

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **5.1 Details or indentification of vulnerabilities of specific system, subsystems or components of:** | | | | |
| 5.1.1 Unclassified systems | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 5.1.2 Classified systems | S | 1.4g | 10 years from date initiated | Could reveal system weaknesses. |
| **5.2 The association of an operating system or other software with a US Army Information System (IS)** | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **5.3 The association of a US Army IS with an Information Assurance Vulnerability Alert (IAVA)** | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **5.4 IAVA patches mitigated through other means; i.e.;, blocked at firewall, Access Control List restrictions, services not running, etc.** | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **5.5 If an IAVA can be applied to fix an open source vulnerability** | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **5.6 If an IAVA cannot be applied and results in a system vulnerability for:** | | | | Mark at level of system because could reveal system weaknesses. |
| 5.6.1 Unclassified Systems | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 5.6.2 Classified Systems | S | 1.4g | 10 years from date initiated | If a system can be instantiated at either the SECRET or unclassified level and vulnerablity is in both, marked at the level of the highest system. |

## SECTION 6 – ADMINISTRATIVE DATA

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **6.1 Media containing PL Net E Information** | See Remarks | | | Mark and handle as per the classification level of the data contained on the system producing the media. Minimum marking will be UNCLASSIFIED//FOUO. Distribution Statement D, FOIA Exemption 4 applies. |
| **6.2 AIM Data** | | | | |
| 6.2.1 AIM Data (Reports which contain Data Products Information) includes, but not limited to:<br>(a) LDIF Report<br>(b) Standard UTO Report<br>(c) AMDWS Load Instructions<br>(d) Tactical Radio Reports (TRRs)<br>(e) Datafiles<br>(f) Readme Files<br>(g) COCOM (Combatant Command) database<br>(h) CONUS (Continental United States) (CONUS) and OCONUS (Outside the Continental United States) Global database<br>Information from databases, documents, or graphics that contain compilations of the following information: IP addresses, system name, role, Unit Reference Number (URN) or user name. | | | | Mark and handle as per the classification level of the data contained on the system producing the media. Minimum marking will be UNCLASSIFIED//FOUO. |
| 6.2.1.1 When not associated with an operational theater and mission | | | | |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 6.2.1.1.1 System/Application Development, and Testing Data | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.2.1.1.2 Production Data (Used for Unit Simulation Analysis) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.2.1.1.3 Production Data (Used for external program testing of interoperability; e.g., AIC) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.2.1.1.4 Production Data (Used for Unit Training Missions in a Non-Combat Operational Area) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.2.1.1.5 Production Data (Used for Application Training) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.2.1.2 When specific data product file references both operational theater and mission | S | 1.4a | Until completion of Unit Operation Mission | Derived from Army ATS SCG, dated September 2014, data element 4.3.3. |
| 6.2.2 Data derived from United States Army Force Management Support Agency for Data Product Usage | See Remarks | | | Mark and handle as per the classification level of the system that created the media. Minimum marking will be UNCLASSIFIED //FOUO. FOIA Exemption 4 applies. |
| 6.2.3 Data derived from FBCB2/JBC-P for Data Products Usage | See Remarks | | | Mark and handle as per the classification level of the system that created the media. Minimum marking will be UNCLASSIFIED //FOUO. FOIA Exemption 4 applies. |
| 6.2.4 Data derived from TNIC for Data Products Usage | See Remarks | | | Mark and handle as per the classification level of the system that created the media. Minimum marking will be UNCLASSIFIED //FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **6.3 TNIC NPD Products** including network configurations, network diagrams, IP spreadsheets, configuration change requests, inter-connectivity diagrams, cut-sheets, load instructions, datafiles and readme files, Field Notices, and Detailed Technical Procedures | | | | |
| 6.3.1 When does not include mission specific password and key information and not loaded on an operational system | U | | | Mark as FOUO. FOIA Exemption 4 applies. Note: IP Templates/Network Configurations products produced by TNIC are unclassified. |
| 6.3.2 When does not include mission specific password and key information and not associated with classified operational theater or mission | U | | | This applies to the template like data products supplied to the unit. |
| 6.3.3 When does include mission specific password and key information and loaded on an operational system | See Remarks | | | Handle at highest classification level of that system or as directed by appropriate SCG. |
| 6.3.4 When specific product file is in use in classified operational theater or mission | S | 1.4a | 10 years or completion of unit mission in operational theater or as directed by appropriate SCG | This does not apply to product files in possession of TNIC since they are not associated with a classified operational theater or mission. |
| **6.4 Production Support Services Data** | | | | |
| 6.4.1 Configuration Control Board (CCB) Resolution Details, Implementation Status | | | | |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 6.4.1.1 All CM documentation, presentations, and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics (where no vulnerability is revealed) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.4.1.2 All CM documentation, for: presentations, and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics (where a vulnerability is revealed) | | | | |
| 6.4.1.2.1 Unclassified Systems | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.4.1.2.2 Classified Systems | S | 1.4g | 10 years from date of document | Derived from Army ATS SCG, dated September 2014. Data element 5.2.6. |
| 6.4.2 Quality Assurance (Analysis, Recommendations includes all quality assurance documentation, presentations, and discussions which reveal system, application, network, software and/or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.4.3 Database Models (all database models which reveal specifications or operating characteristics, unless a case can be made for public release) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.4.4 Application Process Models | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **6.5 Documentation** | | | | This subsection applies to all PL Net E products. |
| 6.5.1 Reports | | | | |
| 6.5.1.1 Reports (all CM documentation, presentations, and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.1.2 Reports (if information reveals a system vulnerability of a classified US Army Information System) | S | 1.4.g | 10 Years or elimination or mitigation of the vulnerability to a low level | Derived from Army ATS SCG, dated September 2014. Data element 5.2.4 |
| 6.5.1.3 Reports (if information reveals a system vulnerability of an unclassiified US Army Information System) | U | | | Mark as FOUO. FOIA Exemption 4 applies |
| 6.5.1.4 System Requirements Analysis (all documents, presentations and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.1.5 Engineering Diagrams (all documents, presentations and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 6.5.1.6 Engineering Presentations (all documents, presentations and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.1.7 System/Application Users Guide (all documents, presentations and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.2 Authority to Operate (ATO) Accreditation Package, including Artifacts | | | | |
| 6.5.2.1 ATO Artifacts which include:<br>(a) System Indentification Profile (SIP)<br>(b) Contigency Plan<br>(c) CM Plan<br>(d) Hardware Software Network Topology<br>(e) Standard Operating Procedures<br>(f) Tempest Review (if unclassified)<br>(g) Memoradums of Agreement, Memorandums of Understanding, Service Level Agreements (MOAs, MOUs, SLAs)<br>(h) RMF Implemenation Plan | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.2.2 ATO Artifacts (which include Plan of Action and Milestones and Scorecard) POA&M for: | | | | |
| 6.5.2.2.1 Unclassified Systems | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 6.5.2.2.2 Classified Systems | S | 1.4g | 10 years from date of determination | Derived from Army ATS SCG, dated September 2014. Data elements 5.2.5 and 5.2.6. |
| 6.5.2.3 ATO Artifacts | | | | |
| 6.5.2.3.1 ATO Artifacts which include ACA report of a classified system | S | 1.4g | 10 years from date of determin-ation | For systems at the classified level, a vulnerability report of an analysis will be classified SECRET. |
| 6.5.2.3.2 ATO Artifacts which include ACA report of a unclassified system | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.3 Application Design (all documents, presentations, and discussions which reveal system, application, network, software and security posture specifications, or operating characteristics) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 6.5.4 Hardware and Software Inventory | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

## SECTION 7 – HARDWARE and SOFTWARE

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **7.1 Hardware Details** | | | | Note: For KMI client node, see NSA/CSS KMI Classification Guide 3-4 |
| 7.1.1 Purpose (Military Use) | U | | | |
| 7.1.2 Nomenclature | U | | | |
| 7.1.3 Model | U | | | |
| 7.1.4 Serial Number | U | | | |
| 7.1.5 Service Tag # | U | | | |
| **7.2 System Configuration** | | | | |
| 7.2.1 IP Address | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.2.2 Media Access Control (MAC) Address | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.2.3 Performance | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **7.3 Servers** | | | | |
| 7.3.1 URL | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.3.2 Purpose (Military Use) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.3.3 Proxy Associations | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.3.4 Public IP Address | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.3.5 Real IP Address | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **7.4 Software Details** | | | | See Section 2.4.5 of this SCG for additional details. |
| 7.4.1 Name | U | | | |
| 7.4.2 Purpose (Military Use) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| 7.4.3 License | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.4.4 Version | U | | | |
| 7.4.5 Nomenclature | U | | | |
| **7.5 Software Configuration** | | | | |
| 7.5.1 Database/Tools Cache Size | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.5.2 Requirements | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.5.3 Application Source Code | See Remarks | | | Protect application source code from unauthoized changes. Classify source code if classified function is included. See NSA classification guidance for classsification of application source code used for the MGC or LCMS. |
| 7.5.4 System Database Scripts | See Remarks | | | Protect database scripts from unauthorized changes. Classify system database scripts if database schema is classified. See NSA classification guidance for classsification of system database scripts used for the MGC or LCMS. |
| **7.6 IAVA or Technical Bulletin** | | | | |
| 7.6.1 Software IAVA Compliance Status | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 7.6.2 Software compliance status of an identified classified system when mitigation is not possible and results in a vulnerability | S | 1.4g | 10 Years from date initiated | Could reveal system weaknesses. |
| 7.6.3 Software compliance status of an indentified unclassified system when mitigation is not possible and results in a vulnerability | U | | | Mark as FOUO. FOIA Exemption 4 applies. |

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **7.7 Login Account** | | | | |
| 7.7.1 Login Account Information | See Remarks | | | Mark as FOUO. FOIA Exemption 4 applies (unless combined with Password, Pin, or Passphrase; then protect login information to the highest level of the protected system). |
| 7.7.2 Account Authorization Level Description | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **7.8 ACES application Crypto Network Plans** | | | | |
| 7.8.1 Black key packages produced by the LCMS or MGC, it include the XML (extensible markup language) metadata | U | | | Note: Mark as FOUO as per NSA/CSS 1-52 classification guidance. Note: LCMS and MGC systems operate as classified systems and all optical media output is classified to the level of the system (SECRET). |
| 7.8.2 ACES application cryptographic network plans, which include all information to establish a communications network | See Remarks | | | Plan will be classified to the level of the network being planned when completed; i.e.; SECRET for SECRET networks; or as directed by appropriate SCG (for example, theater SCG) |

## SECTION 8 – TRAINING, TESTING, and MAINTENANCE

| ELEMENT | LEVEL | REASON | DURATION | REMARKS |
|---|---|---|---|---|
| **8.1 Training** | | | | |
| 8.1.1 Identification and/or location of specialized training specific for the specific system, subsystem or component | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 8.1.2 Training that reveals specific system information (e.g., design, development, capabilities etc.) | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| **8.2 Testing – Specifically User Acceptance Testing (UAT) Testing Documentatiton that reveals no system vulnerablity** | U | | | Mark as FOUO. FOIA Exemption 4 applies. If UAT testing reveals system weakness, see data element 6.5.1.2 of this SCG for guidance. |
| **8.3 Maintenance** | | | | |
| 8.3.1 Association of maintenance equipment or tools that may reveal specific system information | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 8.3.2 Organizational level maintenance | U | | | Mark as FOUO. FOIA Exemption 4 applies. |
| 8.3.3 Intermediate level maintenance | U | | | Mark as FOUO. FOIA Exemption 4 applies. |