



U.S. ARMY

# Cryptographic Modernization Strategy and Requirements

**Mr. Scott Henry**

*Communications Security Branch, Cybersecurity  
Directorate, Office of the Chief Information Officer/G-6*

**22 August 2019**

UNCLASSIFIED





U.S. ARMY

# Agenda

- **Mission and Functions**
- **Key Organizations**
- **Policy and Guidance**
- **Information Systems Security Program**
- **Crypto Modernization Overview**
- **Advanced Cryptographic Capabilities**
- **Crypto Modernization 2 (CM2)**
- **Key Management**

UNCLASSIFIED





U.S. ARMY

# “THE NETWORK IN AN ERA OF GREAT POWER COMPETITION”



## Role as the CIO

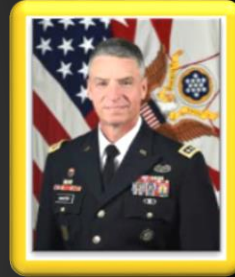
- Reports directly to the Secretary of the Army
- Sets the strategic direction, objectives, and supervises all Army C4 & IT functions
- Capital IT Investment Planning / Budgeting



**POLICY, STRATEGY, GOVERNANCE, PEOPLE**

## Role as the G-6

- Advises the CSA & ARSTAF on operational matters concerning C4IT support
- Supervises Army wide C4/IT activities; defends warfighter critical C4IT resources
- Implements policy and guidance for Cybersecurity



**“Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting.”**

[2018 NDS p. 10]

- Evolution of the Threat (Capability and Intent)
- Relentless Pursuit of Talent

- All Things Data (understand aggregate and visualize)
- Increased speed of decision making

## “The ARMY Network Plan”

**LOE 1**

Modernize the Network (N-CFT)

**LOE 2**

Shape the Force (TRADOC/Cyber COE)

**LOE 3**

Reform Processes and Policies (CIO/G-6)

**LOE 4**

Life-Cycle Sustainment (AMC/CECOM)

**LOE 5**

Security and Survivability (ARCYBER)

## Priority Network Modernization Fixes (2019-2023)

Command Post Mobility & Survivability

Unified Transport Layer

Mission Command Application Suite

Joint / Coalition Interoperability

Cloud



AI



Interoperability



Identity Management



Cybersecurity



EITaaS



IT Investment / Accountability





U.S. ARMY

# COMSEC Branch Mission & Functions

Program and integrate communications security (COMSEC) equipment, key management processes and associated support items of equipment (ASIOE) into the army inventory to secure operational and national level information links and provide users with the means to ensure authenticity, confidentiality and integrity of information. Align policy to current requirement.

- COMSEC Modernization Initiative (CMI)/Obsolescence
- Communications Security (COMSEC) Information Systems Security Program (ISSP)
- National Leadership Command Capabilities (NLCC)
- Sustainment of Key Management Infrastructure (KMI) capabilities
- Key Extension Requests (KER)

UNCLASSIFIED





U.S. ARMY

# Key Organizations

- HQDA Chief Information Officer (CIO)/G-6
- U.S. Army Training and Doctrine Command (TRADOC)
- Program Executive Office Command, Control Communications Tactical (PEO C3T)
- Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR)
- Communications Security Logistics Activity (CSLA)

UNCLASSIFIED





U.S. ARMY

# Policy and Guidance

<b>AR 25-1</b>	Army Information Technology	The Army CIO/G-6 will develop, promulgate, and direct compliance with information security and IA policy (see AR 25-2). The CIO/G6, as the Army Staff G-6, is responsible for information management and signal operations, network and communications security ... will oversee the execution of IM and IT policies and plans by other Army organizations. DCS, G-2 to Operate the U.S. Army Cryptologic Records Center, the repository for all permanent cryptologic records. The Army CIO/G-6 and the DCS, G-2 are strategic partners in transforming Warfighter-required capabilities into standardized, compatible, interoperable, secure, and resourced solutions.
<b>AR 25-2</b>	Army Cybersecurity	This regulation establishes the Army Cybersecurity Program and sets forth the mission, responsibilities, and policies to ensure uniform implementation of public law and Office of Management and Budget, Committee on National Security Systems, and Department of Defense issuances for protecting and safeguarding Army information technology, to include the Army-managed portion of the Department of Defense Information Network, (hereafter referred to as information technology) and information in electronic format (hereafter referred to as information). Information technology includes infrastructure, services, and applications used directly by the Army or for the Army by legal agreements or other binding contracts.
<b>AR 380-40</b>	Safeguarding and Controlling Communications Security Material	Prescribe Army policy and approve procedures for safeguarding and controlling COMSEC material. Ensure that all applicable policies, directives, criteria, standards, and doctrine relating to the safeguarding and controlling of COMSEC material are implemented within the Army.
<b>TB 380-41</b>	Security Procedures for Safeguarding, Accounting and Supply Control of COMSEC	The ARSTAFF (G-3/5/7, CIO/G-6, G-8 and ASA (ALT), and PD COMSEC) with assistance from CSLA conduct the final validation of AISSP equipment requests. In the Army, COMSEC Service Authority responsibilities at HQDA are allocated and executed by the Deputy Chief of Staff, G-2 (Safeguarding and Controlling Communications Security Material), the CIO/G-6 Cyber Directorate, and the Program Director (PD) COMSEC. HQDA G-2 has delegated certain functional Service Authority responsibilities to CSLA as identified on the CSLA website. 3.24.1: The formal CSLA COMSEC Audit/Inspection program is mandated by HQDA G-2 and AR 380-40 to certify and validate central accountability and proper safeguarding and control of COMSEC material.

UNCLASSIFIED





U.S. ARMY

# Policy and Guidance

<b>CJCSI 6510.02E</b>	<b>Cryptographic Modernization Planning (U//FOUO)</b>	This instruction provides policy and guidance for planning, programming, and implementing the modernization of cryptographic products certified by the National Security Agency (NSA) and held by Department of Defense (DoD) Components.
<b>CJCSN 6510</b>	<b>Information Assurance Cryptographic Equipment Modernization Requirements</b>	This notice sets the cryptographic device replacement dates and establishes requirements for the budget planning of modern cryptographic applications and devices in conjunction with risks associated with the cryptographic functions of the device.

UNCLASSIFIED

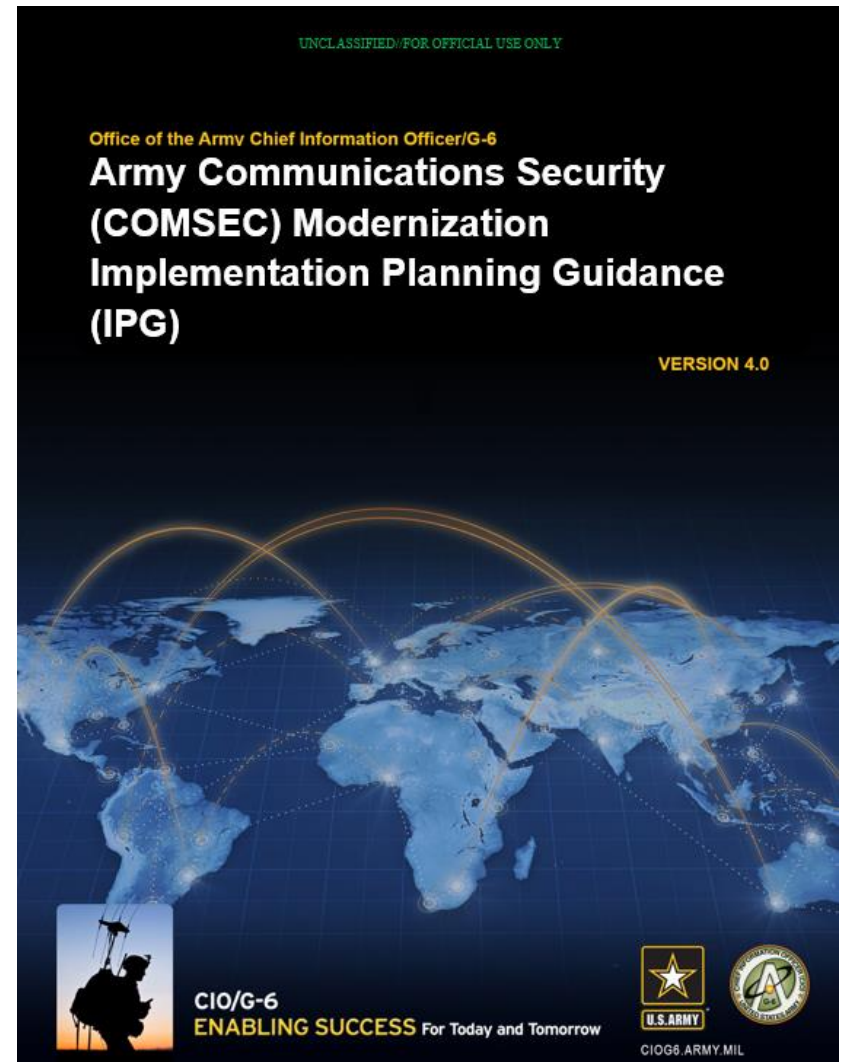




U.S. ARMY

# COMSEC Implementation Planning Guidance

- CIO/G-6 approved on 21 DEC 17
- Informs reader of way ahead for legacy crypto devices
- Contains crypto capability roadmaps
- Currently adjudicating comments from 1-2 Star review



UNCLASSIFIED







U.S. ARMY

# Information Systems Security Program

## ISSP

DoD program through which COMSEC / CYBER requirements are managed in support of the Planning, Programming and Budgeting Evaluation System (PPBES) IAW Public Law 107-347 and the NDAA 2012 for tracking & reporting of modernization efforts

## ISSPA

Army's implementation of the ISSP. Unclassified, web-based application that supports the entry and staffing of all Army COMSEC/CYBER requirements, ranging from COMSEC end items to costs associated with personnel, training, tools, and certification/accreditation requirements

## Functions/Capabilities

- Assists HQDA CIO/G-6 in determining current and future COMSEC/CYBER requirements
- Provides tool to forecast, identify, and allocate resources
- Automates HQDA G-3/5/7, G-6 & G-8 staffing actions for the allocation of limited resources under routine and urgent conditions
- Augments and fills capability gaps in standard logistics systems
- Supports Cryptographic Modernization (CM) efforts
- Supports out-of-cycle changes to MTO&E/TDAs and Operational Needs Statements (ONS)
- Facilitates and tracks COMSEC/CCI loans
- Links COMSEC Accounts/POCs/Department of Defense Activity Address Code (DoDAAC) with requirements
- Allows ACOM/ASCC/DRU to submit projections for future requirements (2 years out)
- Allows the Acquisition Community to forecast COMSEC requirements for Programs of Record

UNCLASSIFIED





U.S. ARMY

# Crypto Modernization

- **What is CM?**
  - CM is a defense capability critical to the success of the Warfighter
  - Provides secure, enduring and continuous communications under current scenarios and emerging threats
  - Transforms cryptographic security capabilities for National Security Systems (NSS) at all echelons and points of use
- **Items affected:**
  - All C5ISR, IT and weapons systems that rely upon cryptography for the provision of assured confidentiality, integrity and authentication services
  - Hardware, software, algorithms, and loading devices to operationalize IA capabilities
  - Link Encryptor Family (LEF), Layer 2/Layer 3 In-line Network Encryptors (INEs), VINSON/ANDVT Crypto Mod (VACM), Secure Voice, Key Management, Tactical Radio
- **Actions to take:**
  - Upgrade/replace cryptographic products to comply with algorithm Last Year of Use (LYOU) dates identified in Chairman of the Joint Chiefs of Staff Notice (CJCSN) 6510, June 2014, Information Assurance Cryptographic Modernization Requirements
  - and Army COMSEC Modernization Implementation Planning Guidance (CM IPG)
  - Near-term emphasis on Link 16, IFF, ACC and Tactical Radio
  - Work with CIO/G-6 to complete Command Plans to plan upgrades/replacements

UNCLASSIFIED





U.S. ARMY

# COMSEC Modernization Drivers

- **Computing power advances (cheaper, more accessible and mobile) have enabled our adversaries and reduced cryptographic product lifecycles**
- **Chairman of the Joint Chiefs of Staff Notice (CJCSN) 6510, June 2014, Information Assurance Cryptographic Modernization Requirements**
  - **Diminishing ability to mitigate risk to extend life of decertified devices**
  - **NSA Advanced Cryptographic Capabilities (ACC) and Cryptographic Modernization standards will make legacy Stand Alone and select radios (embedded) devices obsolete**
- **Technology obsolescence and/or the end of vendor/product support**
- **Network demands for increased capacity (VLAN)**
- **Funding constraints and product availability are impacts to Army Crypto Mod (CM)**

UNCLASSIFIED





U.S. ARMY

# Driving Factors to Modernize

- **Support to the Warfighter – Current & Future Forces**
  - Must field latest technology to the Warfighter as quickly as possible
  - Existing crypto systems do not support emerging network-centric technologies
  - Networks cannot be compromised or “broken” while changes occur
  
- **CJCSN 6510 – CM Plan means different things to different communities**
  - G-3: Operations
  - G-6: Information Assurance
  - G-8: Resources
  - ASA(ALT): Program Development
  - CYBER CoE: Capability Developer and DOTMLPF Analysis for Current and Future Forces
  - C5ISR: Emerging Technologies

UNCLASSIFIED





U.S. ARMY

# Advanced Cryptographic Capabilities (ACC)

- **What is ACC?**
  - ACC is a NSA mandated upgrade of asymmetric cryptographic algorithms providing confidentiality services
  - NSA is the lead for algorithm developments
  - JITC is the lead for testing – first wave of devices currently in Service Lab Testing (vIPer, KG-175D/G, KG-250X/255X)
  - Army is participating in working groups and testing with NSA, JITC and other Services
  
- **Items affected:**
  - Certain Secure Voice Products, In-line Network Encryptors (INEs), Link Encryptors
  - Contact CIO/G-6 for specific products impacted
  
- **Actions to take:**
  - Identify items on the list to receive ACC software update
  - Identify items not on the list that need hardware replacements
  - Work with CIO/G-6 to complete Command Plans to plan upgrades/replacements

UNCLASSIFIED





U.S. ARMY

# Crypto Modernization 2

- **What is CM2?**
  - Extends the original Crypto Mod initiative by updating the U.S. cryptographic inventory with modern capabilities to address current and future threats
  - Integrates new capabilities and alleviate gaps identified in an updated Crypto Mod Initial Capabilities Document (ICD), which is planned for Q1FY20
  
- **Item Affected:**
  - All C5ISR, IT and weapons systems that rely upon cryptography for the provision of assured confidentiality, integrity and authentication services
  - May require physical replacement of a portion of the cryptographic inventory
  
- **Actions to Take:**
  - CIO/G-6 to work with NSA, DoD CIO and the other Services to develop a strategy to upgrade/replace crypto to satisfy CM2 requirements
  - CIO/G-6 to publish Army CM2 strategy in an update to the Army COMSEC Modernization Implementation Planning Guidance (CM IPG)

UNCLASSIFIED





U.S. ARMY

# Key Management Infrastructure (KMI)

- KMI is a JROC approved follow-on solution to the Electronic Key Management System (EKMS) program
- Automated, network-accessible, electronic-based key management and delivery infrastructure that provides the means for secure ordering, generation, production, distribution, management and auditing of cryptographic keys and products
- As the program matures, it will encompass functionality to support key management services to civil agencies, allied and coalition users
- The KMI program is designed to be fielded in multiple Capability Increments (CIs), which includes Spiral and Spin development cycles that will be fielded to Army accounts periodically

UNCLASSIFIED





U.S. ARMY

# KMI Windows 10 Implementation Plan

## ■ Task:

- The DoD Chief Information Officer (CIO), Cybersecurity has tasked the Services to develop a KMI Management Client (MGC) Node WIN10 Implementation Plan by 13 August 19 to meet the DoD CIO mandate of updating the MGC to a WIN10 Platform by March 21
- Establish metrics, timelines, fielding schedule to reach objective state in accordance with HQDA Tasker HQDA-190618-DHQT *“National Security Agency Windows 10 Extension for Key Management Infrastructure”* (see backup slide)

## ■ Objective:

- Gain the CIO/G-6 endorsement to implement the Army’s KMI WIN10 Implementation Plan to meet DoD mandate and improve readiness across the Total Force

## ■ End-Goal:

- Provide the DoD CIO with an Army-approved KMI WIN10 Implementation Plan to field the WIN10 image and improve Army’s operational readiness and maintain a common KMI software baseline

UNCLASSIFIED

16



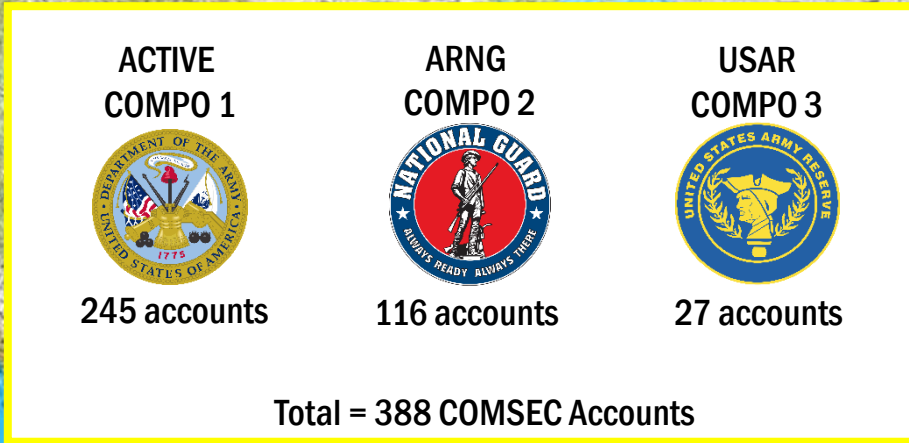




U.S. ARMY

# Army's KMI WIN10 Migration

## Communication Security (COMSEC) Accounts



*Above implementation will put 100% of the Army's COMSEC accounts on a common baseline*

## WIN10 Secure Host KMI S/W Deployment will:

- Meet DoD CIO mandate for WIN10 Secure Host Baseline
- Improve & Strengthen Cybersecurity posture
- Reduce Long-term Security Hardware and O&M Costs (IAVA's / Vulnerabilities)
- Provide Expanded Security Capability
- Improve Reliability, Performance and Increase Bandwidth
- Synchronize with COMPOs (1,2&3) to establish a common KMI Client software baseline

*Implement a detailed plan and structured approach to reach the Objective End State, one standard and one baseline*





U.S. ARMY

# Instructions and Guidance

## National Security Agency Windows 10 Extension for Key Management Infrastructure (14 JUN 19)



CHIEF INFORMATION OFFICER

DEPARTMENT OF DEFENSE  
8000 DEFENSE PENTAGON  
WASHINGTON, D.C. 20301-6000

JUN 14 2019


MEMORANDUM FOR NATIONAL SECURITY AGENCY/CENTRAL SECURITY  
SERVICE, CHIEF INFORMATION OFFICER

SUBJECT: National Security Agency Windows 10 Extension for Key Management  
Infrastructure

Reference: National Security Agency Memorandum "Key Management Infrastructure  
Windows 10 Extension Request," 1 May 2019

The DoD Chief Information Officer (CIO) concurs with the National Security Agency's request and approves the Windows 10 extension through March 2021 with the exception of the 31 afloat accounts. The afloat accounts will be completed as soon as possible, but no later than March 2023. Also, within 60 days of the date of this memorandum, the Services will publish their Windows 10 implementation plans. Services will submit their Windows 10 implementation plans to the DoD Deputy CIO for Cybersecurity, Cybersecurity Enterprise Planning and Capabilities Integration Directorate.

The point of contact for this matter is Mr. Larry Randal, [larry.l.randal.civ@mail.mil](mailto:larry.l.randal.civ@mail.mil), (571) 372-8466.

  
Essye B. Miller  
Principal Deputy

cc:  
Chief Information Officer, Department of the Army  
Chief Information Officer, Department of the Navy  
Chief Information Dominance and Chief Information Officer, Department of the Air Force  
Deputy Chief Information Officer, Department of the Navy (Marine Corps)  
Deputy National Manager for National Security Systems

UNCLASSIFIED





U.S. ARMY

# KMI Status

- **The Army current KMI baseline is Spiral 2, Spin2**
  - IAW HQDA EXORD “to be released” all Army accounts are required to upgrade their KMI MGC system to KMI Spiral 2, Spin 3, Maintenance Release (MR) 3 which includes Window 10 (WIN10) Operating System (OS) no later than March 2021
  - DoD CIO has mandated that all KMI accounts (Service and Agency) will upgrade to WIN10 NLT March 2021 unless deployed (Memo: 14 June 2019)
  - All Army accounts that do not upgrade and do not have an approved waiver from HQDA CIO/G-6 will be closed
  
- **In FY19 zero units requested KMI training during the 2018 Structure Manning Decision Review (SMDR). This caused a major shortage for KMI Operating Account Manager (KOAM) and COMSEC Account Manager Course (CAMC) availability**
  - Contact your unit training team so that they may properly project your training requirements for KMI and CAMC
  - Ensure your KMI Account has sufficient personnel to operate at all times
  - Plan ahead for departing Solders and get replacements trained in advance

UNCLASSIFIED





U.S. ARMY

# Questions



CIO/G-6 COMSEC milSuite Site: (Scroll down to COMSEC)

<https://www.milsuite.mil/book/community/spaces/cryptomod/ciog6-portal>

CryptoMod Portal: <https://www.milsuite.mil/book/community/spaces/cryptomod>

NSA IA Library (SIPRNET):

[https://www.iad.nsa.smil.mil/resources/library/cryptomod\\_section/index.cfm](https://www.iad.nsa.smil.mil/resources/library/cryptomod_section/index.cfm)

UNCLASSIFIED





U.S. ARMY

# Contact Information

## **KMI POC:**

Mr. Major Lambert, [major.lambert7.civ@mail.mil](mailto:major.lambert7.civ@mail.mil), 703-545-1733

Mr. Stephen Gonzalez, [stephen.s.gonzalez2.ctr@mail.mil](mailto:stephen.s.gonzalez2.ctr@mail.mil), 703-545-1677

Ms. Tracey Floyd, [tracy.d.floyd.ctr@mail.mil](mailto:tracy.d.floyd.ctr@mail.mil), 703-545-1706

Mr. Eric Saloy, [eric.j.saloy2.ctr@mail.mil](mailto:eric.j.saloy2.ctr@mail.mil), 703-545-1607

## **RM:**

Ms. Amber Payton, [amber.n.payton.ctr@mail.mil](mailto:amber.n.payton.ctr@mail.mil), 703-545-1702

Mr. Greg Sanders, [gregory.e.sanders2.ctr@mail.mil](mailto:gregory.e.sanders2.ctr@mail.mil), 703-545-1737

## **Crypto Modernization:**

Mr. Scott Henry, [scott.k.henry3.civ@mail.mil](mailto:scott.k.henry3.civ@mail.mil), 703-545-17178

Mr. Steve Schless, [stephen.e.schless2.ctr@mail.mil](mailto:stephen.e.schless2.ctr@mail.mil), 703-545-4617

Mr. Ray Nelson, [raymond.l.nelson18.ctr@mail.mil](mailto:raymond.l.nelson18.ctr@mail.mil), 703-545-1696

Mr. John Couillard, [john.a.couillard.ctr@mail.mil](mailto:john.a.couillard.ctr@mail.mil), 703-545-1717

Ms. Pattie Rimbey, [patricia.m.rimbey.ctr@mail.mil](mailto:patricia.m.rimbey.ctr@mail.mil), 706-791-6388

UNCLASSIFIED

