PORTFOLIO

PEO★C3N

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

TABLE OF CONTENTS

PEO C3N

The U.S. Army Program Executive Office Command, Control, Communications, and Network (PEO C3N) develops, acquires, fields and supports the Army's Unified Network (Tactical and Enterprise) to ensure force readiness in both current missions and potential future large scale combat operations. This critical Army modernization priority delivers resilient terrestrial and satellite communications capabilities to ensure commanders and Soldiers remain connected and always informed, even in the most austere and hostile environments.

PEO C3N is delivering an integrated Unified Network to regions around the globe, enabling high-speed, high-capacity voice, data and video communications to an Army user base that includes joint, coalition and other mission partners.

With so much riding on the communications of people and systems, Army senior leaders have designated the network as the No. 1 priority in the Army's transformation effort, calling for systems that are more simple, intuitive, low-signature and iterative. In 2024, the Army implemented Command and Control (C2) Fix to 1) "Fix" the network to be ready for the next fight, 2.) Make our command post smaller and more survivable, though just as capable, and 3) Push more complicated network management to division and above, simplifying technology at the edge to keep Soldiers focused on the fight.

To ensure the network and its myriad radios, blue force tracking, command post, fires support technologies, satellite systems and other capabilities meet these requirements, the Army's C2 Fix effort is identifying specific units to experiment with near-term networked communications systems designed to counter the threats leaders see evolving on the battlefield. Known as "transforming in contact," this experimentation is becoming an increasingly critical component for evaluating and helping to refine technologies that could be needed at a moment's notice. U.S. Army Forces Command (FORSCOM) is supporting these assessments by providing a mix of light and armored formations across brigade combat teams, divisions and enablers.

The Army's Next-Generation (NGC2) effort is next, focused on prototyping and experimentation, using a new and more adaptive approach to data centric tools for the commander to increase the Army's competitive advantage.

JTNC

The Joint Tactical Networking Center (JTNC) is a support organization to the Services, the DoD Chief Information Officer (CIO), the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), the Joint Staff J6, and USD Research and Engineering (USD(R&E)).

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

JTNC
JOINT TACTICAL NETWORKING CENTER

DESCRIPTION

The JTNC enables secure, interoperable, and resilient tactical communications capabilities aligned to modular open architectures in support of Service, Multi-Service, and Coalition forces. JTNC core functions include maintaining a cyber-hardened DoD Information Repository (IR); providing technical analyses and capability characterizations on tactical communications products; providing open systems architecture standards; and serving as waveform technical advisor to the Command, Control, and Communications Leadership Board (C3LB). The JTNC is leveraging commercial vendor information exchange opportunities to help drive DoD comms resiliency. The JTNC is leading the HF Interoperability and Architecture Sub-Working Group (HF I&A SWG), which is intended to enable interoperable DoD HF radio services to include chat and email functionality. The JTNC serves as technical advisor to DoD CIO, and is responsible for providing oversight of Lead Service activities and assisting in the identification and resolution of cross-service networking disconnects.

CAPABILITIES

*   DoD Information Repository (IR): The JTNC maintains a cyber-hardened DoD IR to provide controlled access for proprietary and non-proprietary waveforms and associated network managers, operating environment software, models, architectural standards, application program interfaces, and future tactical communications products. This serves to protect and distribute code and documentation based on legal agreements between government and software developers.
*   Joint Communications Marketplace (JCM) is an online portal and DoD collaboration space for vendors to showcase their tactical communications products. JCM provides acquisition authorities the capability to conduct market research on emerging technologies, informed by Government analyses that may incorporate JTNC capability characterization results.
*   JTNC Capability Characterization process has been developed for commercial off-the-shelf /non-developmental item tactical communications products. JTNC's Capability Characterization verifies and validates a product's performance against developer-stated specifications to provide a report on the innovative technologies and capabilities.
*   Modular Radio Architecture (MRA) will expand the Government's ability to develop affordable, secure and standardized tactical communications products. The MRA is intended to address emerging networking scenarios, while utilizing the necessary interfaces to maximize interoperability. MRA establishes open systems architecture to facilitate the integration of technology.
*   Technical Analysis: The JTNC performs waveform analyses, Waveform Assessment for System Milestone Review, conformance evaluations, and capability characterizations on tactical communications products to assessing which products meet their advertised capabilities and align with DoD wireless communications, interoperability, and cybersecurity standards and policies.
*   Exportability Analysis and Licensing Review: The JTNC analyzes potential exportability of tactical communications products and provides recommendations as needed. JTNC reviews software defined radios and waveform export license requests, submitting findings to DoD CIO. The JTNC supports service and various DoD agencies, overseeing the protection of critical technologies of wireless com- munications exported under com- mercial, direct commercial sales, and/ or foreign military sales and licenses/ agreements.

A-C | JTNC enables interoperable, secure and resilient waveform and wireless communications by recommending standards, conducting technical analyses, and maintaining a DoD Information Repository.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

NGC2

Command and Control (C2) is foundational to warfighting, and lessons learned from recent support to contingency operations in Ukraine and Israel, as well as threat assessments in the INDOPACOM AoR, show that the Army's current C2 information systems should be modernized to meet commanders' needs for large scale combat operations against near peer adversaries.

PEO ✭ C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PEO C3N

DESCRIPTION

Current mission command systems are not mobile, intuitive, or survivable enough to easily overcome the current threat, changes in the character of warfare, and the pace of technology. As part of the Army's continuous transformation effort, initiatives are being implemented to transform how the Army operates, trains, and equips for C2 capabilities that enhance its lethality, mobility, and survivability in large-scale combat as part of the Joint Force. The Army's operational imperative is to improve systems responsibly, using innovative solutions from units and industry; at the same time, preparing for the future by ensuring the next generation of C2 systems are built on a portfolio of capabilities that effectively address emerging threats and ensure dominance over adversaries.

The Army's Next Generation Command and Control (NGC2) portfolio of capabilities will provide commanders with the ability to make more, better, and faster decisions through advanced analytics, an integrated data layer, open architecture, and robust and resilient transport. The result is data-centric C2 at every echelon that can operate in any environment.

NGC2 requirements are currently being informed by persistent experimentation. Market research and prototyping will create a competitive environment for innovative industry partnerships and continuous integration of new technologies.

KEY POINTS:

- NGC2 is a vision for a fundamentally different way to rapidly identify requirements and fill gaps using persistent experimentation with rapidly evolving and maturing technologies such as cloud, artificial intelligence, and cybersecurity along with stronger industry partnerships that enable integration of dual use capabilities.

- NGC2 is focused on advancing open and modular architecture, data-centric design, ease of use, scalability across the force, and enabling warfighter mastery of evolving C2 software, supported by survivable and flexible network transport. The desired end state is an intuitive, adaptive software architecture that provides access to operational data and enables commanders to effectively exercise C2 at echelon, make faster decisions, and synchronize and manage combat power across all warfighting functions.

A ǀ U.S. Army Chief Warrant Officer 3 Cole Brown, assigned to the 2nd Cavalry Regiment, checks communication signal on Tactical Mission Data Platform during Brave Partner exercise on Ramstein Air Base, Germany, Nov. 30, 2023.

B ǀ Spc. Brantley Tercero, a fire support specialist assigned to the 10th Mountain Division Artillery, trains using the Advanced Field Artillery Tactical Data System Artillery Execution Suite during Command Post Exercise 1D, Aug. 14, 2024, on Fort Drum, New York. The Army's Next Generation Command and Control (NGC2) portfolio of capabilities will provide commanders with the ability to make more, better, and faster decisions through advanced analytics, an integrated data layer, open architecture, and robust and resilient transport. The result is data-centric C2 at every echelon that can operate in any environment.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

BECS

Product Director Base Emergency Communications System (BECS) supports installation force protection, public safety, installation management, and homeland security. BECS manages, engineers, acquires, delivers, and supports CONUS non-tactical Land Mobile Radio (LMR), Computer-Aided Dispatch (CAD), Next Generation 9-1-1 (NG-911), First Responder Broadband Network (FRBN) and Enterprise Mass Warning Notification (EMWN).

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PM IEN
INTEGRATED ENTERPRISE NETWORK

DESCRIPTION

BECS integrates, modernizes, standardizes, and enhances the Public Safety Communication emergency architecture to align with the Common Transport Layer and Services infrastructure within the greater Unified Network. BECS provides mission command to emergency assets to coordinate response to emergency incidents.

CAPABILITIES

Land Mobile Radio (LMR) is the Army's primary voice capability for first responders. LMR provides secure, portable communications; network coverage on/off Army cantonment areas, housing and training areas, and standalone facilities; and interoperability with mission partners.

Enterprise Mass Warning Notification (EMWN) provides the ability to produce, track, and disseminate information through network alerts, beacons, Giant Voice (outdoor speakers), and telephone alerts for at-risk military communities experiencing no-notice threats, hazards, and other emergencies.

Next Generation 9-1-1 (NG-911) includes Call Handling System (CHS), infrastructure, Geospatial Information System (GIS), and Location Information Services (LIS).

NG-911 CHS enables operators and dispatchers to receive Call For Service (CFS) from a person needing emergency response. CHS supports calls routed from Army telephone networks and commercial (non-government) sources via NG-911 Emergency Services IP Network (ESInet) to automatically deliver 9-1-1 calls to the designated Army Public Safety Answering Point (PSAP).

Computer-Aided Dispatch (CAD) receives incident data from 911 and other types of CFS; assists the dispatcher in determining the optimal response; and provides dispatch and ongoing incident management support. In addition to NG-911 CHS, CAD systems can interconnect to a variety of approved external sub-systems such as records management systems, LMR, and mobile computing devices, via the First Responder Broadband Network.

A I **Justin Calixto, OCONUS APM PD BECS, conducts LMR System Acceptance Testing for Southwest Asia, Jordan.**
B I **Christian Ross, PSAP Modernization APM PD BECS, conducts PSAP walk-through and brief to BG Camilla White at Aberdeen Proving Ground, MD.**
C I **Clive Flores, LMR APM PD BECS, and Fort Liberty LMR team conducted a Ribbon Cutting Ceremony 31 May 2024, signifying the completion of Fort Liberty's LMR Modernization.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY
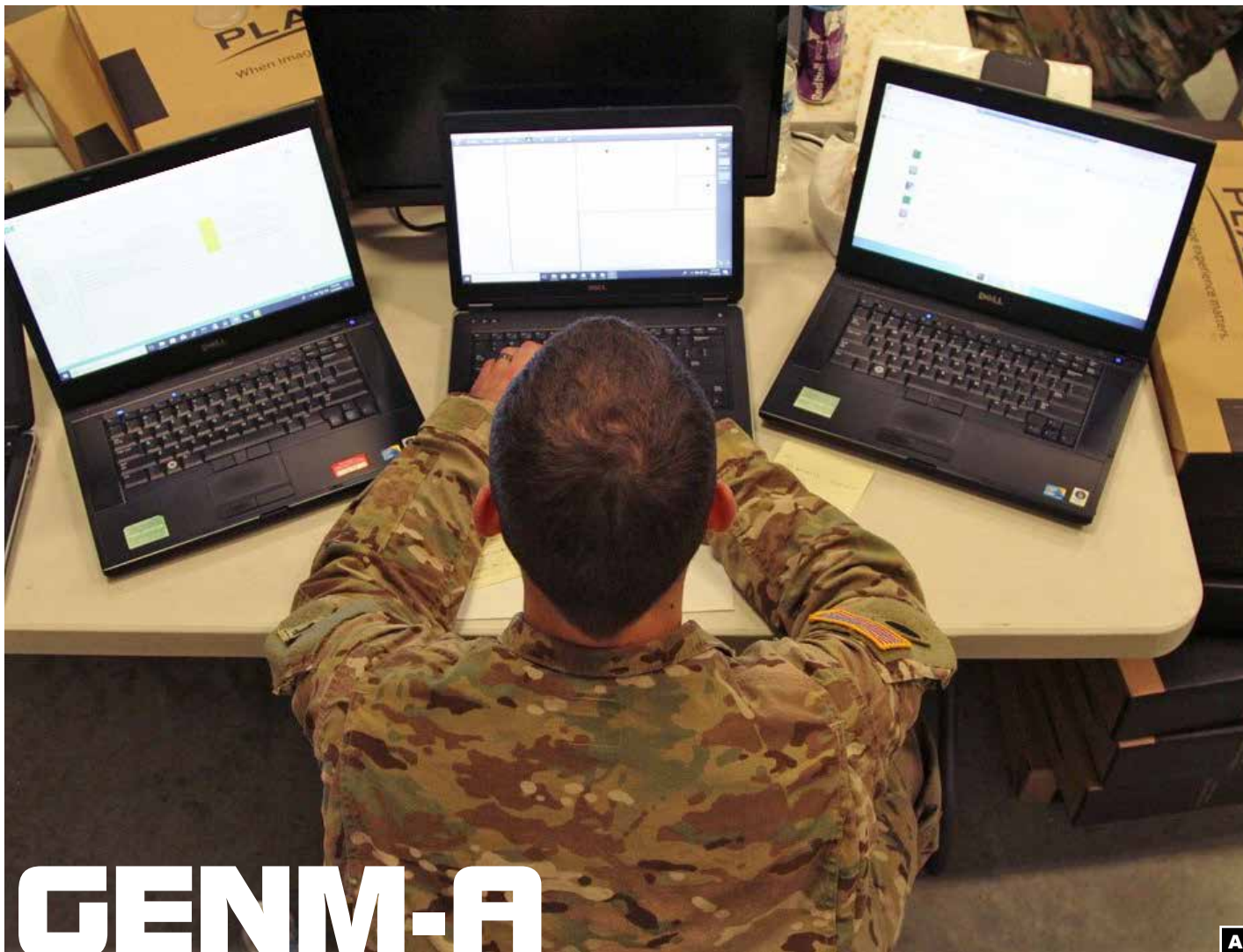
GENM-A

A

Global Enterprise Network Modernization – Americas (GENM-A) conducts network, information, and infrastructure modernization projects at bases, posts, camps, and stations (B/P/C/S) throughout the Continental United States (CONUS).

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PM IEN
INTEGRATED ENTERPRISE NETWORK

DESCRIPTION

GENM-A's network modernization capabilities include network services, voice services, inside plant and outside plant upgrades, as well as video modernization. The organization's technology innovation capabilities include the evaluation of new technologies for potential incorporation into GENM-A's Installation Campus Area Network (ICAN) model. GENM-A is also the responsible program office for the implementation of standardized capabilities for home station mission command centers, as well as infrastructure services for strategic command centers at Army and Army-supported command centers.

MISSION AREAS

Technology Innovation: Identify, validate, and integrate commercial technologies into the Army network, including SIPR modernization and WiFi baseline integration.

Network Architecture Modernization: Update the Army Army Base/Post/Camp/Station (B/P/C/S) architecture to enable Unified Network Operations through modernizing classified and unclassified data and voice networks.

Network Infrastructure Modernization: Enable successful network architecture modernization by upgrading the Army B/P/C/S network infrastructure components.

CAPABILITIES

Comprehensive Network Modernization (COMPMOD)

- Non-Secure Internet Protocol Router (NIPR) modernization
- Secure Internet Protocol Router (SIPR) modernization
- Foundational Wi-Fi
- Inside Plant (ISP)
- Outside Plant (OSP)
- Mission Command from Afar (MCfA)
- Installation Service Node (ISN)
- Army Enterprise Transport (AET)

Global Secure Network (GSN)

- Enables SIPR connectivity globally from all theaters
- Streamlines SIPR user experience
- Enables scalability, flexibility, and survivability
- Delivers Commercial Solutions for Classified Programs (CSfC), Virtual Desktop Infrastructure (VDI), and Multiple Independent Levels of Security (MILS)

Voice Modernization (VMOD)

- Voice services to modernize Army B/P/C/S voice infrastructure to an Everything over Internet Protocol (EoIP) technology
- Decommissioning of Time Division Multiplexing (TDM) voice systems
- Provides Army B/P/C/S IP-based local voice management solutions
- Facilitates the divestiture of legacy technology

A ׀ Army Sgt. Kyle Plumley, an intelligence analyst for Joint Force Headquarters, works three laptop computers at Camp Atterbury, Ind. The Army Futures Command is enabling Army personnel at Aberdeen Proving Ground, Maryland, to remotely access classified networks via their commercial internet.
B ׀ Soldiers of 67th Expeditionary Signal Battalion, 35th Theater Tactical Signal Brigade prepare CISCO switches for installation as part of the Network Modernization (NETMOD) program.
C ׀ GENM-A installs an IP-based voice system at Fort Leonard Wood to replace the TDM technology.


ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

GENM-O

Global Enterprise Network Modernization – OCONUS (GENM-O) is the Army's total lifecycle acquisition manager chartered with delivering modernized, classified and unclassified infrastructure, voice, video, data and command center capabilities that are scalable, accessible, flexible, and defensible.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PM IEN
INTEGRATED ENTERPRISE NETWORK

DESCRIPTION

GENM-O's delivery of modernized infrastructure, voice, video, data, and command center capabilities aligns with the Army's Network Modernization Strategy and Army Unified Network Plan (AUNP) to both home station and deployed forces in the Africa Command (AFRICOM), Central Command (CENTCOM), European Command (EUCOM) and Indo-Pacific Command (INDOPACOM) areas of operation.

MISSION AREAS

Technology Innovation: Identify, validate, and integrate commercial technologies into the Army network, including SIPR modernization and WiFi baseline integration.

Network Infrastructure Modernization: Enable successful network architecture modernization by upgrading the Army's OCONUS network infrastructure components.

CAPABILITIES

Global Enterprise Network Modernization (GENMOD)

- Non-Secure Internet Protocol Router (NIPR) modernization
- Secure Internet Protocol Router (SIPR) modernization
- Foundational Wi-Fi
- Inside Plant (ISP)
- Outside Plant (OSP)
- Mission Command from Afar (MCfA)
- Installation Service Node (ISN)
- Army Enterprise Transport (AET)

Army Global Unified Network

- Enables Global User Mobility
- Aligned to DOD Zero-Trust Architecture
- Reduce Infrastructure and O&M Cost
- Lower Latency for Services and Applications

Voice Modernization (VMOD)

- Voice services to modernize Army voice infrastructure to a Voice over Internet Protocol (VoIP) technology
- Decommissioning of Time Division Multiplexing (TDM) voice systems
- Facilitates the divestiture of legacy technology

A ▎ Building mounted Cisco wireless antennas provide network connectivity to buildings not currently serviced by fiber optic cable.

B ▎ Telecommunication rooms and associated racks, power and grounding, heating, ventilating, and air conditioning (HVAC), cable management, and hardware (core/distro/edge switches).

C ▎ Trench digging to install fiber optics for high-speed secure connections between buildings and to network switch racks supports ICAN's outside portion of an installation's campus area's telecommunication infrastructure and includes installing fiber optics cabling and associated accessories between networked buildings.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

WESS

Wideband Enterprise Satellite Systems (WESS) manages the acquisition, fielding, and lifecycle sustainment of strategic satellite communication and satellite control systems for the Department of Defense, enabling critical communications for the National Command Authority, Combatant Commands, Defense Agencies, and International Partners.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PM IEN
INTEGRATED ENTERPRISE NETWORK

CAPABILITIES

- Wideband SATCOM Operational Management System, a suite of planning, monitoring, and management tools that enable US Space Force, Space Operations Command to plan, provision, and manage satellite communications missions for DOD users.

- Modernization of Enterprise Terminals, a large aperture fixed-station satellite terminal operating in the military X and Ka bands.

- Digital Communications Satellite Subsystem, a suite of modems, switching, routing, encryption, precision timing, and management tools interconnecting the DOD Information Network over satellite.

- Senior National Leadership Communications, a suite of satellite communications providing a direct communications link for crisis communications between the National Command Authority and the President of the Russian Federation.

A ı **WESS develops the management and control tools to operate DoD's WGS satellites from five Wideband SATCOM Operations Centers.**

B ı **Satellite baseband systems provide the switching and routing infrastructure to connect Army and DoD networks over satellite for global reach.**

C ı **AN/GSC-52B(V) Modernized Earth Terminals provide DoD with access to the Wideband Global SATCOM network at more than 40 teleport facilities and missile defense sites globally.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

CPMOD

In alignment with the Army's top priorities for C2FIX and network modernization, the CPI2 program will transition to the Command Post Modernization (CPMod) program in FY25. This change more accurately reflects the PdM's current mission of supporting Army Network direction and strategic objectives. The program continues to tackle mobility, scalability and survivability of Army command posts. The program incorporates the five components of mission command—personnel, networks, information systems, process and procedures, facilities and equipment—integrating emerging technologies and leveraging Soldier feedback from experimental units.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PROJECT MANAGER INTEGRATION
PM 125
INTEROPERABILITY SERVICES

DESCRIPTION

PdM CPMod addresses the challenges posed by contemporary and future land conflict, such as physical signatures, mobility, and standardization. Command post designs for this effort are integrating approved commercial off-the-shelf (COTS), government-off-the-shelf (GOTS) systems, and government programs of record (PoR) that support command post operational needs.

The CPMod program is comprised of four product lines, CPI2 Increment 0, Command and Control On The Move (C2OTM), Mounted Integrated Tactical Network (M-ITN) and Command Post Modularity. The increased mission responsibility streamlines mobile command and control (C2) efforts within the PEO, ensuring a coordinated and effective System of System approach to modernizing Army command posts and command post platforms. CPMod will continue to assess and address command post modularity by improving current designs and influencing future requirements.

The CPI2 Inc 0 program is post Milestone C and is being fielded to multiple Army units. The program utilizes feedback from Soldiers to make improvements to the Family of Medium Tactical Vehicles (FMTV) baseline. In the coming year, PdM CPI2 will field two more Army divisions with the Inc 0 solution. C2OTM will continue to equip three priority divisions with tailorable and modular on the move solutions to enhance their mission readiness. The Integrated Tactical Network (ITN) will continue to deliver an integrated package of PoR and COTS solutions to multiple formations and unit types, converging the concepts of ITN and C2OTM into a standardized package. All these efforts enable greater C2 of Army units, increasing lethality and survivability.

CAPABILITIES

- CPMod leverages improvements in technology to reduce the current CP footprint and improve mobility / survivability. Through the integration of approved and fielded mission command information systems, GOTS and COTS technology CPMod ensures the operational needs of the division, brigade and battalion CPs are addressed.

- CPI2 Inc 0 utilizes the FMTV to host integrated workspaces while enabling commanders with the ability to rapidly disperse. The centerpieces of CPI2 Inc 0 are the Mission Command Platform (MCP) and Command Post Support Vehicle (CPSV) which serve as user workspace and server / communication platforms.

- C2OTM provides mobile and modular transit-case based solutions which can be easily moved between platforms or shelters while maintaining beyond line-of-sight communications. Additionally, select Army platforms within M-ITN formations receive an integrated C2OTM platform compatible with the M-ITN architecture. This allows commander's maximum flexibility on the battlefield and improves survivability through mobility.

- M-ITN integrates a modernized communication, command and control package into multiple Army vehicles across all echelons of the force. These packages replace outdated stove-piped systems with a System of System network architecture, streamlining C2 across the formation.

- Command Post Modularity seeks to upgrade CPI2 Inc 0 platforms to make a more dismountable/modular solution as well as address future requirements.

A-C ∣ Soldiers with the 1-2 Stryker Brigade Combat Team (1-2 SBC) conduct the CPI2 Limited User Test (LUT), at Joint Base Lewis-McChord, WA, in August 2023, where they tested future command and control capabilities integrated into various vehicle platforms designed to reduce the current command post footprint and improve mobility and survivability. All these efforts enable greater C2 of Army units, increasing lethality and survivability.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

CHS

Common Hardware Systems (CHS) acquires and supports sustainment of highly flexible, cost-effective, common, and simplified non-developmental, commercial information technology (IT) solutions that improve interoperability and connectivity on the battlefield, while garnering efficient competition to enable the latest commercial technology solutions to meet tactical and operational requirements.

PEO C3N

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PROJECT MANAGER INTEGRATION
PM I2S
INTEROPERABILITY SERVICES

DESCRIPTION

Army Regulation 25-1 Army Information Technology identifies CHS as the mandatory source for the procurement of commercial IT hardware for tactical/operational requirements. As such, CHS coordinates across tactical programs, providing consolidated procurement and sustainment support of commercial IT hardware including non-developmental and modified commercial off-the-shelf (COTS) items. The program portfolio continually updates new contract items ensuring modern, emerging technologies are available to enable overmatch capabilities for warfighters.

The CHS office maintains a procurement contract to execute their mission in support of tactical and operational requirements. From receipt of requirements to award of a corresponding delivery order for a supported program, CHS averages a 90-day processing time with an expedited capability available to meet urgent needs.

CHS also provides the government with an increased ability to perform supply chain risk management, critical function analysis of components, critical program information assessments and implementation of other protection measures contained in program protection plans. This contract feature protects the network and strengthens the Army's cybersecurity posture.

CHS includes a pre-negotiated pricing schedule for the life of the contract with quantity discounts; additional warranty options with up to eight years of coverage providing a 72-hour turnaround time; incentives to provide the lowest price hardware; and the ability to procure technical documents based on competitive pricing.

CAPABILITIES

- **Rapid Acquisition**: Centralized approach to contracting streamlines ordering process, reduces time between order and delivery, and allows for economies of scale in pricing.

- **Design & Engineering**: Provides direct customer support throughout the development of new capabilities, assists in the design of hardware configurations, facilitates hardware evaluations, and informs the selection of common hardware solutions.

- **Lifecycle Management**: Provides warranty options, failure analysis reporting, worldwide 72-hour repair, and warranty/repair tracking.

- **Configuration Management**: Maintains the configuration of equipment for the life of the contract or until the product is going End-of-Life/End-of-Sale.

- **Ruggedization**: Provides modified commercial IT hardware for tactical/operational use in accordance with MIL-STD-810 to ensure product survivability in austere conditions.

- **End-of-Life Management**: Coordinates with customers who previously procured items that have gone End-of-Life/End-of-Sale to determine future needs and identify suitable replacements.

- **Bonded Storage**: Provides for up to one year of bonded storage for any customer.

A ǀ A Soldier uses a CHS ruggedized device in the field.
B ǀ The Tactical Control Console is the primary interface for the AN/VIC-5 system.
C ǀ A Soldier assesses his mission using CHS equipment during Enroute Mission Command exercise.
D ǀ A Soldier configures operational transit cases.

I-CAM

Identity, Credential and Access Management (ICAM) is the foundation for the Army's Zero Trust Roadmap and continued cybersecruity modernization. The Army established ICAM efforts to identify exactly who and what is operating on the network, and what data they are accessing, to ensure no users or assets are provided implicit trust based solely on their physical or network location.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

UNO's ICAM software is composed of both enterprise and tactical operating environment, which enables a user to access to resources whether they are operating at the enterprise or tactical environment. Tactical (T-ICAM) and Enterprise (E-ICAM), when combined, create a single ICAM capability.

CAPABILITIES

E-ICAM

- The E-ICAM solution provides services for a user identity directory, granular identity governance, access management, privileged access, and Multi-Factor Authentication (MFA).

- The application officially launched for FY25, allowing the program to begin migrating large Army systems into the system to eliminate stove-piped and disparate ICAM systems currently implemented throughout the Army.

- E-ICAM establishes a single set of authoritative user identity data and providing a global integrated ICAM platform to manage user access across cloud, on-premises, and supports denied, disconnected, intermittent, and support limited (DDIL) environments when connected on all classification levels.

T-ICAM

- T-ICAM is a Software Pathway program that modernizes how Person Entities (PEs) and Non-Person Entities (NPEs) authenticate to and access the tactical network. It enables a greater degree of security for the tactical network, ensuring that that network is available when the commander needs it to operate, congested, contested, battlefield.

  - T-ICAM leverages the authoritative identities that already exists on the Enterprise ICAM style to apply them in a tactical environment.

- ICAM Services will be bundled together in a common framework and be distributable and deployable at the point of need across the Army's Unified Network (UN) and federated with DoD and Mission Partner ICAM capabilities to the greatest extent possible to ensure the Warfighter is provided with a consistent user experience regardless of the operational conditions within the UN.

A ׀ The Army's ICAM services are securing privileged users from the threats of modernday attackers.

B ׀ The Army is creating a Unified Network that is secured by a zero-trust architecture, which will require users to be authenticated, authorized, and continuously validated for security configuration and posture to access applications and data

C ׀ The new E-ICAM is the first modernized architecture to support the Army's Zero Trust initiative. Migration of large Army systems is underway, which eliminates the stove-piped and disparate ICAM systems currently implemented throughout the Army.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

NIM

Product Manager Network Integration and Modernization (PdM NIM) formally assigns staff and resources to manage technical integration in support of the Army's network modernization. The product office works across multiple PEOs to promote synergy in planning, execution, risk management, and serves as a touch point for systems engineering, design, integration, and testing.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

PROJECT MANAGER
INTEGRATION
PM
I2S
INTEROPERABILITY SERVICES

DESCRIPTION

PdM NIM's support aligns to the Army's objective to define the minimum essential network capability required at echelon to fight and win in a LSCO environment. PdM NIM supported network design, development, testing, and fielding to Infantry and Stryker brigade combat teams throughout FY21 – FY23, with added support to divisioncentric network designs in FY24. PdM NIM is now supporting the Army's three new focus areas for Command and Control (C2) On the Move, Next Generation C2, and Electronic Signature Management. After completing a preliminary design for FY24 C2 FIX network designs, PdM NIM is implementing an even more iterative, agile approach, still backed by acquisition rigor, Soldier experimentation and feedback, and industry and S&T alignment, to identify formation and echelon appropriate network designs.

PdM NIM executes 6.4 (Prototype & Experimentation) budget activities that support advanced component development activities aligned to the Army Network Modernization Priority. PdM NIM supports integrated technology/prototype system evaluations and technology demonstrations of commercial technologies via Technical Exchange Meeting (TEM) contracts and S&T projects which, upon successful completion, will transition to either existing programs or new programs for integration and fielding.

FOCUS AREAS

• PdM NIM manages the PEO C3N Network Baseline Process incorporating the latest feedback from Army Experimentation efforts (C2 FIX), PM versioning upgrades, and updates to Army requirements ensuring that tailored architecture designs for specific units are interoperable and functioning prior to being fielded to a unit.

• PdM NIM supports Next Generation Command and Control through 6.4 funding alignment and managing the PEO C3N S&T process thereby ensuring future Army innovations are properly scoped, resourced, and are able to mature to their program of record transition partners.

A ‖ **PdM NIM supports the Army's C2 Fix initiative, which was tested during the 101st Airborne (Air Assault) Joint Readiness Training Center (JRTC) at Fort Johnson, Louisiana, in August 2024**

B ‖ **PdM NIM provided critical support to division-centric network designs throughout FY 2024, including to the 25th Infantry Division during its Joint Pacific Multinational Readiness Center rotation in November, 2023.**

C ‖ **PdM NIM's supported the Army's C2 Fix effort, which focused on C2 On the Move capabilities, enabled Soldiers to reduce the command post footprint and their electronic signature.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

TNIC

Tactical Network Initialization and Configuration (TNIC) rapidly delivers relevant network initialization products and solutions to the warfighter in support of evolving Army directives. Data Products are a collection of mission data required to initialize the tactical network and command and control (C2) applications. This data includes the information required to enable end-to-end network-centric connectivity and interoperability across the tactical internet (TI), such as internet protocol (IP) addressing, unit reference numbers (URNs), router, switch and firewall configurations, and more. Data Products are used to instantiate the digital systems. Once loaded, they populate look-up tables and local databases, and are expected to be maintained within the runtime operational environment by the systems utilizing the data or by the network manager responsible for that system.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

The information within Data Products is used to populate address books; create default message lists; determine communication protocols between systems; and determine how a system processes and handles information from another system. Every PM that touches the tactical network needs Data Products to establish the network layer and enable binary messaging protocols, such as Variable Message Format (VMF) and United States Message Text Format (USMTF) in support of the common operating picture (COP), situational awareness (SA) and command and control (C2) messages for Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, Reconnaissance (C5ISR) applications. All systems internal and external to PEO C3T who meet these criteria need Data Products.

CAPABILITIES

- **Command Control/Application (C2/Apps) Initialization:** Provides critical components that enable system-of-system interoperability for software applications that would otherwise be incompatible; assigns, manages and deconflicts Unit Reference Numbers (URN); generates address books and other application-specific data bases as required.

- **Initialization Tool Suite (ITS):** A capability fielded to units that allows them to add, modify, and delete data in their fielded data products to ensure the digital architecture is configured optimally to support the mission as it evolves through the phases of operation.

- **Network Initialization:** Provides critical components that enable system-of-system interoperability for the Army's tactical network; assigns, manages and deconflicts tactical Army IP address space for NIPR, SIPR, MPE and Colorless (private, public and multicast); assigns and manages autonomous system numbers (ASN), Global Block Numbering Plans and telephony; generation of network device configurations (i.e., router, switch and firewall) and unit specific IP plans.

A ı Initialization products provide the technical glue to ensure the components of the overall network are able to function together in a manner consistent with current and future warfighter requirements.
B ı The 50th Expeditionary Signal Battalion-Enhanced and 63rd Expeditionary Signal Battalion conducted a combined Large Scale Combat Operations (LSCO) communications exercise on Fort Bragg, North Carolina.

UNO

The Unified Network Operations (UNO) program focuses on integrating and converging the The Unified Network Operations (UNO) program is a key enabler for resilient secure global data exchange and the Army's on-going network modernization efforts, such as a zero trust security architecture. These tools make it easier for Signal Soldiers (S6/G6) from the tactical edge up through Corps to plan, configure, manage, monitor, control and secure/defend their tactical network assets.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

UNO provides a centralized management and control capability that allows the Army to manage and operate its networks more effectively, while also improving network security and resiliency. It is a key enabler within the Unified Network Plan, which outlines the Army's strategy for modernizing and integrating its networks to support a wide range of mission-critical operations.

The UNO program is moving towards a singular, intuitive user interface, where Soldiers will be able to conduct endpoint management at a single device that can reach out to all their unit's different network nodes. This will allow for more streamlined and efficient network management, as well as improved situational awareness and security. The initial integrated suite of software applications for the UNO program aims to integrate existing network operation tools into a simplified, user-friendly capability. This will enable Signal Soldiers - from the tactical edge up through Corps (S6/G6), to plan, manage, monitor, configure, and secure the Army's

UNO utilized the Middle Tier Acquisition (MTA) pathway to develop and prototype NetOps tools, while supporting Army network modernization goal, and conducting risk reduction efforts for the UNO Program of Record (POR). In 2024, UNO transitioned to multiple software acquisition pathway efforts to rapidly develop prototype and eventually deliver UNO capabilities.

While in the software acquisition planning phase, the program office initiated a competitive prototyping down-select process, which is a way for the UNO program to identify and evaluate the best commercially available solutions for use in the Army's

networks. The UNO competitive prototyping process is a key part of the Army's network modernization efforts and will help to ensure that the Army has access to the most advanced and effective network management and security tools available.

CAPABILITIES

• **Unified Net Ops (UNO)**: Lower Tier Tactical and Upper Tier Tactical are executing Competitive Prototyping, which is a process that allows for the demonstration and evaluation of commercially available solutions in a lab environment. In phase 1, commercially available solutions will be demonstrated and evaluated to conduct a competitive down-select going into Phase 2 of Competitive Prototyping. In Phase 2, selected tools will improve their technologies in an Agile, DevSecOps environment in conjunction with multiple Operational Assessments. Soldier feedback will be incorporated into the design and evaluation process.

• **Ruggedized Applications Platform -Tactical Radios (RAP-TR)**: Combines several software applications to a single tactical network management tool to plan, configure, load, and monitor legacy waveforms and advanced networking waveforms in current and future tactical radios. Atom – an easy-to-use, single radio planning and loading tool that supports all of the Army's tactical radios and four advanced/legacy waveforms simultaneously.

• **Integrated NetOps Battalion and Below (INB2)**: Monitors and manages the LTT radio network.

A ׀ UNO will enable Soldiers to sense, control, and visualize the Unified Network, from both a targeted and holistic perspective, to enable real-time assessment of impacts to joint multi-domain operations
B ׀ Soldiers train on mobile ad hoc network (MANET) radios during the Army's Operations Demo Phase II, conducted during the 2d Cavalry Regiment's Dragoon Ready 2023 operational exercise in Hohenfels, Germany, in February 2023, which provided an opportunity for Soldiers to train on multiple software defined radios.
C ׀ A Soldier operates the UNO software, which provides a common operating picture that allows Soldiers in the command post to track every single radio on the network, during the Army's Operations Demo Phase II, conducted during the 2d Cavalry Regiment's Dragoon Ready 2023 operational exercise in Hohenfels, Germany.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

A

FSC2

Fire Support Command and Control (FSC2) empowers Army, joint and coalition commanders to plan and execute the delivery of both lethal and non-lethal fires and effects with the capability to enhance situational awareness and increase collaboration.

PEO C3N

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

FSC2 systems comprise the entire sensor-to-shooter digital kill chain, from the dismounted forward observer through theater and Combatant Command planning cells. These systems integrate Army, joint and coalition targeting capabilities and fuse that information with the ballistic calculations required to deliver precision munitions.

CAPABILITIES

- **Advanced Field Artillery Tactical Data System** (AFATDS) **Artillery Execution Suite** (AXS) is a modernized Fires Execution software suite that will provide the same fully automated support for fires execution as AFATDS but will be designed using a Modular Open System Approach to produce a data-centric, open architecture Fires solution. AFATDS AXS will displace the currently fielded AFATDS 6.8 baseline. AFATDS AXS, sub-products at echelon (Fire Support, Technical Fire Direction, and Tactical Fire Direction), combines essential situational awareness data, intelligence information, and targeting data in near real-time to make effective targeting decisions that align with Next Generation Command and Control (NGC2) Mission Command guidance and priorities. It pairs targets to weapons to provide optimum use of fire-support assets and timely execution of fire missions.

- The **Joint Targeting Integrated Command and Coordination Suite** (JTIC2S) software will provide critical fires/targeting capability for joint and organic Army fire support management, and a joint fires/targeting common operational picture (COP) for joint and coalition partners, as well as at echelon for target development. JTIC2S will replace the Joint Automated Deep Operations Coordination System (JADOCS) capability and will enable commanders to functionally integrate targeting efforts in a federated method.

- Military service branches at echelon will utilize the functions within JTIC2S for a synchronized targeting tactical picture with Army and Joint Fires COP to support Joint All Domain Command and Control (JADC2) and Multi Domain Operations against a near-peer adversary.

- AXS and JTIC2S will share a common Fires Safety Critical Baseline back end infrastructure within NGC2.

- Precision Fires-Dismounted (PF-D) is used by forward observers and fire support teams to transmit and receive fire support messages over standard military line-of-sight, high-frequency and satellite communications radios. PF-D enhances this functionality over legacy systems with a revamped user interface and precision fires targeting capabilities. PF-D is hosted as a software application on common Army hardware in the Handheld Computing Environment.

- Fires capabilities in sustainment include the Lightweight Forward Entry Device, which hosts the Forward Observer System software, enabling mounted forward observers and fire support officers to plan, control and execute fire support operations at maneuver platoon, company, and battalion and brigade levels across the mounted formation; the Profiler weather system, which improves artillery accuracy by providing meteorological data, one of five requirements for accurate predicted fires; CENTAUR, the lightweight technical fire direction system that provides an automated cannon ballistic firing solution to the Fire Direction Centers; and the JADOCS, a joint mission management software application that provides a suite of tools and interfaces for integration across battlespace functional areas focusing on the Joint Target Cycle.

A | A 155mm artillery round is fired from a 777 Howitzer by the 101st Airborne Division during its JRTC rotation in August 2024.

B | A Targeting Officer from III Corps G2 provides user feedback during usability testing of the Joint Targeting Integrated Command & Coordination System (JTIC2S) in November 2024 at Fort Cavazos, Texas.

C | Soldiers from the 10th Mountain Division Artillery learn how to navigate the AFATDS AXS on a tablet during a Soldier Touch Point, August 2024. With the new software, Soldiers can use AFATDS AXS on various platforms without being tethered to specific hardware, enabling mobile command and control.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

A

MMC

The next generation of JBC-P, known as Mounted Mission Command (MMC) modernizes the existing JBC-P software and hardware utilizing a phased approach with three Lines of Effort under the MMC Family of Systems: MMC-Software (MMC-S), MMC-Transport (MMC-T), and MMC Computer System.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

MISSION COMMAND
EFFECTIVE//AGILE//DECISIVE

DESCRIPTION

The foundation to which all MMC products are designed is based on open standards that promote competition and enable rapid injection of new technology and capability. As part of the Mounted Computing Environment (MCE) – one of six computing environments that make up the Army-wide Common Operating Environment (COE) – MMC provides all the movement and maneuver applications, as well as a number of essential Warfighting Functions (WfFs) to include Integrated COP, Intel, Fires, Engineering, Medical, and Logistics. MMC also allows for integration of third-party applications that provide additional functionality via the MCE software convergence architecture and infrastructure.

MMC leverages proven, Army investments – the JBC-P hardware and network – and has been deployed as a software-only upgrade to replace JBC-P software. MMC-S will operate on future MMC-T hardware (next-generation transceivers and encryption devices) to bolster product security and network resiliency to outpace adversarial countermeasures and threats. MMC provides a common user-experience that enables leaders to lead and fight within their formations from anywhere on the battlefield. MMC-S was approved for full deployment in October 2023. It was assessed at the Initial Operational Test & Evaluation as Effective, Suitable, and Survivable in April 2023. MMC-S has deployed on non-integrated platforms as a software-only upgrade via a simple hard drive swap on the existing Mounted Family of Computer Systems hardware infrastructure.

Convergence partners leverage the infrastructure and services of MCE to develop WFF capabilities without having to build a complete system from the ground up – resulting in stream-lined integration, hardening, accreditation and critical capabilities that are rapidly delivered to the Warfighter.

CAPABILITIES

- Enables Mission Command On-The-Move by providing an environment for an integrated suite of platform-based mission command applications and services
- COTS-based application framework that is the same as the Dismount maneuver systems that are built on Android for a simplified / intuitive user experience with embedded help functions for reduced training burden on multiple form-factors
- Governing standards and common software for common look and feel across the Army COE enabling critical cross-cutting capabilities
- Provides a Software Development Kit framework and infrastructure that enables an application development hosting environment of all WfFs and rapid integration of third-party software
- Improved Situational Awareness through tactical symbology, graphics, and overlays
- Improved Command and Control through tactical messaging, chat, instant message, and free text
- Improved on and off-road vehicle navigation with steer-to capability and route planning
- Over-the-air updates for maps, software, security patches, and network keys
- Multi-Band path diverse networking with APACE and Smart Routing across enterprise and tactical transport for full System of System COP federation (4G LTE, WiFi, Iridium, etc.)
- Increased on-board and off-board sensor and weapons integration via open standard interfaces
- Assured – Position, Navigation, and Timing (A-PNT)

A | Soldiers with the 2nd Brigade Combat Team, 101st Airborne Division (Air Assault) operate the Mounted Family of Commuter Systems (MFOCS) running the Mounted Mission Command-Software (MMC-S) system during the Joint Readiness Training Center (JRTC).

B | U.S. Army Advisors, assigned to the 1st Security Force Assistance Brigade review communication systems during Operation Combined Victory (OCV) as part of a communication exercise at Camp Atterbury, Indiana, Feb. 4, 2024.

C | Screenshot of MMC-Software

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

S2I

Secure Signals Infrastructure (S2I) designs, develops and deploys cyber capabilities to the Army to establish cyber operational overmatch.

DESCRIPTION

S2I delivers capabilities to Army Service Component Commands (ASCCs) through divisions at the tactical edge that allow warfighters to understand and depict cyberspace while defending friendly key cyber terrain. S2I's agile acquisition and integration processes achieve both near- and long-term capability development to ensure dominance in the cyber battlefield.

CAPABILITIES

- **Tactical Defensive Cyberspace Operations** (DCO) **Infrastructure** (TDI): Cyberspace defenders have the need to locally and remotely protect friendly tactical cyber terrain, maneuver in and across tactical enclaves, and counter cyber adversaries to ensure the reliability of critical tasks and services. TDI provides users with active hunt and defense tools to protect against cyber-attacks in the tactical network. The TDI system is physically and logistically converged with the Tactical Server Infrastructure (TSI) to minimize size, weight, and power (SWaP) requirements at Divisions and above.

- **Tactical Cross Domain Solution** (TCDS): A critical component in military and defense operations, enabling secure, real-time sharing of information across different security domains. TCDS provides the Army a capability that enables information and communications to be shared and transmitted across different security domains in austere tactical environments. TCDS is a Low Size, Weight, Power and Cost (SWaP-C),

rugged, tamper-resistant cross domain solution ideal for use in ground vehicles, mobile shelters, ground sensor systems, aircraft and UAVs.

- **Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance/Electronic Warfare** (C4ISR/EW) **Modular Open Suite of Standards** (CMOSS) **Mounted Form Factor** (CMFF) **Mounted Common Infrastructure** (MCI): CMFF-MCI will provide the Army a capability that will converge communication, situational awareness, and positioning, navigation, and timing (PNT) capabilities into a single CMOSS compliant form factor (chassis) mounted on selected military platforms that can be employed on an operational environment. This capability will easily and rapidly equip ground vehicles and aviation platforms with capabilities like PNT, electronic warfare (EW) protection and others, through capability cards plugged into a common chassis. The CMFF Chassis will include smart display for user interface, including converging tactical communication waveforms; Mission Command applications; Assured Positioning, Navigation, and Timing (APNT); and Force Protection.
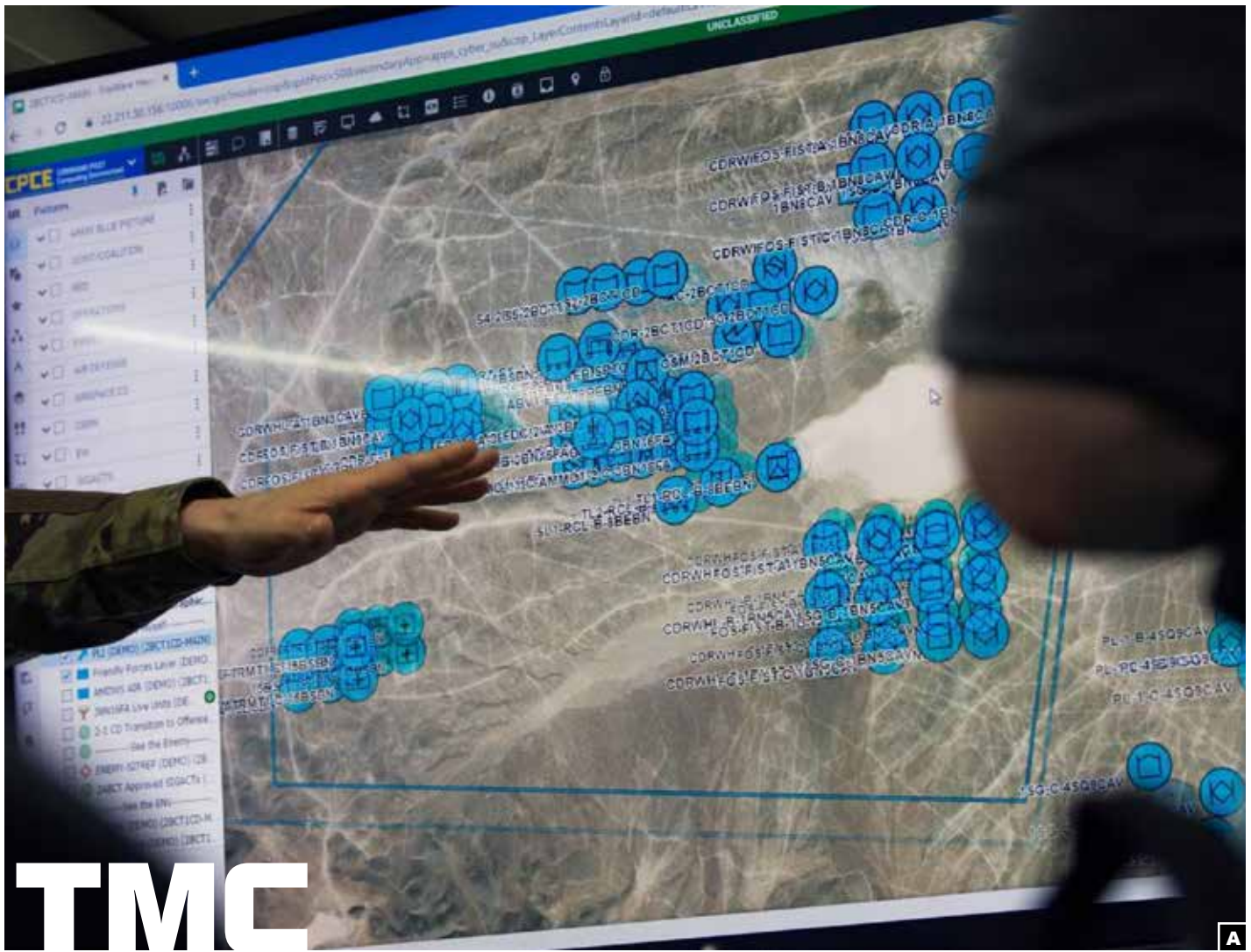
A | Soldiers are taking part in a Tactical Defensive Cyber Operations Infrastructure (TDI) user jury at Aberdeen Proving Ground (APG). As part of continued Developmental Operations (DevOps) activity across the U.S. Army, PdM S2I invited six network defenders from the 82nd Airborne Division to leverage their feedback in TDI's development.

B | CMFF – MAJ Nathaniel Titus, MMC-T A/PM, utilizing Mounted Mission Command Software deployed on an I/O Single Board Computer (SBC) Capability Card integrated into the CMFF MCI chassis during the Network Modernization Exercise (NETMODX), at Joint Base McGuire-Dix-Lakehurst (JB MDL).

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

TMC

A

Product Manager (PdM) Tactical Mission Command (TMC) provides the Army with an integrated mission command capability across command post and platforms, through all echelons, and provides core services and applications, and warfighter functionality in the areas of fires, logistics, intelligence, airspace management and maneuver.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

MISSION COMMAND
EFFECTIVE//AGILE//DECISIVE

DESCRIPTION

TMC provides a software and server hardware framework (common interface, data and services) upon which warfighter applications can be converged and future applications can be built. TMC provides an integrated, interoperable, cybersecure and cost-effective computing infrastructure framework for multiple warfighting functions. TMC provides programs of record (PoRs) with a core infrastructure, including a common operating picture (COP) tool, data persistence, common applications such as mapping and chat, common hardware configurations and common user interface. This effort eliminates duplicative or redundant implementations, speeds up and simplifies future development efforts and enhances interoperability and data sharing across multiple echelons.

CAPABILITIES

- **Command Post Computing Environment** (CPCE) delivers an easy-to-use common operational picture (COP) through a single mission command suite operated and maintained by soldiers. CPCE offers a common geospatial solution (map) and common data services, including an extensible database and data persistence, obtained through the Tactical Data Platform (TDP). The system is designed to reduce the training burden on Soldiers.

- **Tactical Server Infrastructure** (TSI) is the foundational server baseline that hosts CPCE and provides critical common services. Future development of the server infrastructure referred to as the Cloud Enabled Modular Infrastructure (CEMI), will support both Army and COTS cloud integration. CEMI is developed with open industry standards supporting Warfighting Functions

WfFs and service consolidation onto lightweight software containers, which will increase infrastructure security, reduce hardware resource consumption, and provides a container development ecosystem that servers can operate as a cloud edge node while reducing license cost.

- **Tactical Data Platform** (TDP), with first instance fielded in 1QFY25, enables data ingress/egress, synchronization, and management of coordinated data sets for visualization. TDP provides access to various enterprise data sets with the ability to map to a common, extensible, and Multi-lateral Interoperability Program (MIP)-based data model. The data platform tools are currently hosted on the TSI with synchronization to Master Data Nodes and Tactical Data Nodes at Division, Corps and Army Service Component Command (ASCC). TDP will function as the path forward for convergence of WfF data.

- The latest **Tactical Server Infrastructure**, or TSI, hardware is being fielded to units receiving CPCE. More than 270 units have been fielded TSI systems. TSI systems provide various improvements over the legacy Battle Command Common Services server stacks including an 800-pound weight reduction, a 50 percent reduction in setup and teardown time, and a reduction in the number of transit cases from nine to three, significantly increasing agility. The TSI will continue to modernize and improve size, weight, and power attributes as commercial server technology improves.

A ı **PEO C3N personnel highlight recent Command Post Computing Environment enhancements during a demonstration at Joint Base Myer-Henderson Hall.**
B ı **Soldiers complete Command Post Computing Environment training during the Mission Command Training Program at Fort Leavenworth, Kansas.**
C ı **During JWA21, a U.S. led multi-national division conducted tactical operations in a live, virtual and constructed environment, where the Army conducted operational assessments on several network capabilities managed by PEO C3N, including two critical to coalition interoperability – the CCE network enclave and CPCE software. The Army flexed these systems in the Mission Partner Environment and injected an operational threat with contested cyber and electromagnetic activities.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

TRANSPORT-AT THE HALT

Tactical Network Transport At The Halt (TNT-ATH) enables global command and control and robust voice, video, and data communications anywhere on the planet. TNT-ATH leverages a combination of high-capacity line-of-sight (radio) and beyond-line-of-sight (satellite) communications nodes for multipath diversity and resiliency in contested environments. These robust network communications systems operate at-the-halt and at-the-quick-halt (ATQH) and deliver the real-time data that commanders need to make rapid informed decisions. To support expanding network requirements and improve the readiness of today's operational force, the Army continues to modernize the TNT-ATH capability, improving deployability, mobility, computing power, and interoperability, while optimizing and increasing bandwidth and resiliency in congested and contested environments.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

The current/legacy TNT-ATH portfolio contains three main transportable network nodes that provide high-speed wide area network capability for secure voice, video and data exchange. The **Tactical Hub Node** (THN) supports division and above headquarters; the **Joint Network Node** (JNN) supports brigade and above headquarters; and the **Command Post Node** (CPN) supports battalion-level headquarters and smaller-sized units.

Project Manager Tactical Network (PM TN) has been delivering the **Network Integration Technology Enhancement** (NITE) since fiscal year 2021 to refresh and enhance the Army's widely fielded legacy JNN and CPN equipment, which is reaching end of life. The modular NITE solution provides a more than 200 percent increase in computing power, while reducing size, weight and power (SWaP) and equipment setup time for increased mobility.

NITE Modernization Re-designs enhance the TNT-ATH baseline even further and significantly reduce SWaP-Cost and Soldier burden, while increasing simplicity, network security and resiliency, operational flexibility, maneuverability and command post survivability.

- **Medium Communications Node-Tactical (MCN-T)** – replaces the CPN: The smaller more capable MCN-T was fielded to the first unit in FY23. For fast ATQH operations, Soldiers can pull over and rapidly power up their MCN-Ts in the back of a vehicle using vehicle power.

- **Large Communications Node-Tactical (LCN-T)** – replaces the JNN: On the current timeline, PM TN expects to begin fielding to brigade and division headquarters in FY26. LCN-T is a smaller version of the JNN with a new shelter that can be integrated onto a JLTV. Since LCN-T will be transit case-based, units can deploy the system without the shelter.

SATCOM Capabilities: Current/Legacy Satellite Transportable Terminals (STTs) operate in conjunction with JNNs and CPNs. Future modernized capability will be known as the Large Deployable Terminal (LDT) and will be part of the SATCOM FoT.

Scalable Network Nodes (SNNs) -- support Expeditionary Signal Battalion-Enhanced (ESB-E) and other expeditionary formations and replaces all of the legacy JNN, CPN, STT, and Single Shelter Switch (SSS) equipment items within a formation with a single equipment kit. The smaller footprint and reduced complexity enables ESB-Es to increase their Command Post support, while reducing transportation requirements by over 60 percent.

Extra Large Deployable Terminal (XLDT) -- replaces the THN: As part of the SATCOM FoT, PM TN will modernize the current THN design, which consists of the Unit Hub Node (baseband) and the Unit Hub Satellite Truck. This will result in a multi-band BLOS capability for division and above, with a sizable reduction in SWaP.

A ǀ A U.S. Army Soldier from the 86th ESB leverages ATH network capability at Project Convergence Capstone 4, Camp Pendleton, California in February 2024.
B ǀ PM TN conducted two Soldier-driven NITE logistics demonstration events for theLCN-Tv1 Omega shelter and the MCN-Tv2., at Fort Hood, Texas, in April 2023.
C ǀ Spc. Jamil Ahmed, a multichannel transmission systems operator-maintainer with the 248th Aviation Support Battalion, Maryland NG, sets up a secure internet protocol phone at Camp Grayling, Michigan.
D ǀ Soldiers from the 50th ESB-E, 35th Corps Signal Brigade, set up SNN equipment during a field training exercise at Fort Bragg, N.C.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

TRANSPORT-ON THE MOVE

A

Integrated on a variety of tactical vehicles to best suit unit requirements, Tactical Network Transport-On The Move (TNT-OTM) configurations enable Command and Control On-The-Move (C2 OTM) and robust voice, video and data communications while mobile from any location on the battlefield. TNT-OTM enables Soldiers operating in remote and challenging terrain to maintain network communications while on patrol, with connectivity similar to that of a stationary command post. Using both line-of-sight and beyond-line-of-sight for optimal network connectivity, these configurations deliver a global, mobile, resilient tactical communications network.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

TNT-OTM's mobility ensures effective and less predictable offensive and defensive operations. In the fires battalions, the system improves the speed and reliability of the fires network, while also extending range and increasing the survivability of artillery units. Soldiers can expand operational reach well beyond line-of-sight radio ranges and still maintain voice, chat, and data communications using satellite-based re-transmission. Retrans can be located with maneuver forces alleviating the need for isolated retrans elements that require combat power to protect.

TNT-OTM is currently integrated on a variety of tactical vehicles including Mine Resistant Ambush Protected (MRAP) platforms, Strykers, Humvees, and they will be integrated onto the Joint Light Tactical Vehicles (JLTVs) that will eventually replace the Army's fleet of Humvees. Additionally -- working alongside PdM Command Post Integrated Infrastructure (CPI2) at Project Manager Interoperability, Integration and Services (PM I2S) -- PdM Mission Network will support the second phase of the Armored Formation Network OTM Pilot in FY25 and will help integrate modernize OTM final design solutions into armored formations to enable these lethal units with more effective and less predictable offensive and defensive operations.

Mobility is a crucial element to survivability in any future conflict. This is especially true for the C2 OTM that commanders need to make and execute rapid informed decisions. With this in mind, the Army's evolving network will arm commanders with resilient secure OTM network connectivity to enable uninterrupted data exchange, C2, a single common operating picture and enhanced situational awareness.

CAPABILITIES

Tactical Communications Node-Lite (TCN-L) provides satellite and line-of-sight network connectivity, both on-the-move in a convoy, at the quick halt, and to the stationary command post, enabling mission command and advanced communications.

Network Operations and Security Center-Lite (NOSC-L) provides network management and enhanced tactical network planning, administration, monitoring and response capabilities. The hardware is located on the vehicle and is connected by cables to the laptops and large display screens inside the tactical operations center where the communications officers manage the network.

Points of Prescence (PoPs) are installed on select combat platforms at corps, division, brigade and battalion echelons, enabling mobile mission command by providing on-the-move network connectivity, both line-of-sight and beyond-line-of-sight. The PoP enables mobile mission command by providing on-the-move network connectivity, both line-of-sight and beyond-line-of-sight.

Soldier Network Extensions (SNEs) are installed on select vehicles to provide on-the-move network communications to extend the network from the battalion down to the company level. Using its on-the-move satellite communication systems, the SNE can also be used to heal and extend lower echelon tactical radio networks for geographically separated elements blocked by terrain features.

Armored Formation Network On The Move (AFN OTM) will provide battalion and above echelons line-of-sight and beyond-line-of-sight with modern networking technologies for today's battlefield. It will enable secure mission command, enhance fires coordination, increase network resiliency, and provide multiple data paths to Army Mobile Command Posts.

A-D ǀ The Program Executive Office Command, Control, Communications, and Network (PEO C3N) supports the 1st Infantry Division command post exercise (CPX) at Fort Riley, Kansas, in November 2024, where the unit leverages its newly integrated network on-the-move capabilities in preparation the Army's Armored Formation Network On The Move (AFN OTM) Pilot II, later in FY25. To support the pilot, the Army previously integrated commercial OTM prototype capabilities into some of the unit's Joint Light Tactical Vehicles (JLTVs) and HUMVEEs.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

RHN & GAIT

A

The Army's large fixed-installation Regional Hub Nodes (RHNs) support theater-level operations. The regionally located RHNs enable global network connectivity to securely transport information both within theater and around the world. RHNs support joint training and real-world contingency operations, as well as humanitarian, disaster relief and national emergency response. Additionally, through the Global Agile Integrated Transport (GAIT) design, commands with dispersed units around the globe can maintain mission command and network operations capabilities from their home station or forward- deployed headquarters.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

The GAIT network design creates a global network mesh that enables secure high-capacity voice, video and data exchange, mission command and network operations between Army formations located around world. This dynamic architecture provides multiple routing path options and solutions, enabling a more robust, resilient and expeditionary network. GAIT interconnects the Army's RHNs and multiple DoD satellite communication gateways worldwide to enable integrated global network transport. Units can also transport data directly between hundreds of these fixed enduring GAIT Points of Presence routers located around the globe, to simplify network transport pathways. These network routers are installed at fixed military locations, such as corps, division, theater tactical signal brigades and special user home stations. This simplifies network transport even further and enhances multipath diversity for a more resilient network.

GAIT delivers a more unified and robust network, enabling current expeditionary network capabilities and laying the groundwork for future network transport innovation. GAIT is a cornerstone in the Army's network modernization efforts, posturing the service to meet its near and long-term goals in support of Large Scale Combat Operations against advanced enemies. GAIT enables commanders to execute mission command and make faster decisions by enabling a unified network transport for mission command systems and the integration of those systems and their server stacks between home station and forward deployed locations. This unified integration enables near real-time common operating picture that commanders can

trust. It will also support the Army's future cloud computing initiatives.

Future Multi-Domain Operations will require an expeditionary force that is ready to fight the battle as soon as boots hit the ground. Before deploying to contingency, support or training missions, Army and Marine Corps units can leverage GAIT from their home station to complete the long list of networking configuration and policy tasks needed to connect to overseas coalition networks and conduct integrated mission command. Commanders and their units can also practice on mission command and signal integration in the forward theater before they deploy, and participate in coalition meetings and battle update briefs, increasing unit proficiency ahead of the fight.

CAPABILITIES

- Enables global network connectivity to transport information both within theater and out around the world.

- Enables home-station mission command and network operations with forward deployed units.

- Complex networking configuration and policy tasks needed to connect to overseas coalition networks and conduct integrated mission command can be completed at home-station so Soldiers can connect once they hit the ground.

- Cornerstone in the Army's network modernization efforts, such as tactical cloud capabilities.

A । The extensive satellite communications capabilities of RHNs enable regionalized reach-back to the Army's global network.
B । Chief Warrant Officer Two Felix Salinas, 54th Signal Battalion (front), discusses Defense Information Systems Agency and RHN convergence with Lt. Gen. Patrick D. Frank, Commanding General, U.S. Army Central (left), at the Central Command RHN on December 28, 2023.
C । Project Manager Tactical Network continually upgrades and modernizes the RHN network components, seen here at the Continental United States East RHN.

EMC

Enroute Mission Command (EMC) provides short notice units, such as the XVIII Airborne Corps, with the critical in-flight mission command and plane-to-plane/plane-to-ground network communications they need to be successful in joint forcible entry operations.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

EMC improves the Army's ability to combat sophisticated threats by enabling commanders to continue to refine their products and plan the mission as they approach their objective, receiving the critical intelligence they need to be effective and lethal. This suite of network communications capabilities provides commanders with the same mission command capabilities they would use in a command post on the ground, in essence, turning the plane into a flying command post.

Units like the XVIII Airborne Corps' Immediate Response Force must be able to rapidly deploy anywhere in the world with little notice and with as much situational awareness as possible. By leveraging technologies similar to those used by today's commercial airlines to provide inflight internet access, EMC enables these units to access mission command capabilities, all from an Air Force C-17 aircraft. Because of the increased bandwidth the system provides, commanders enroute to an objective can tap into mission command applications and utilize services such as Secure Voice over Internet Protocol phone calls, chat and email.

Additionally, EMC capabilities increase the reliability of unit communications between aircraft. Soldiers operating EMC can extend the same enroute communications, enhanced situational awareness and planning capabilities to other planes that are flying to the mission, enabling all forces to remain synchronized.

MAIN COMPONENTS

- The **Fixed Installed Satellite Antenna** (FISA) provides tactical network connectivity on select Air Force C-17 aircraft. Once EMC's FISA is integrated onto a C-17 aircraft, Soldiers merely roll-on the other EMC equipment, and roll it off at the end of the mission. Project Manager Tactical Network fields and manages the EMC equipment for the Army and is working with the Air Force to transition the current C-17 Ku-band (commercial satellite) FISAs to commercial Ka-band; this upgraded capability is known as the Fuselage Mount Antenna (FMA). The commercial Ka-band provides dedicated bandwidth, improved service, and better worldwide coverage at a comparable cost.

- The **Key-leader Enroute Node** (KEN) provides airborne units with broadband reach-back data capability; intra-aircraft data and voice communications with subordinate units, Secure Video Teleconferencing and SVoIP, plane-to-plane and plane-to-ground communications between task force commanders and combatant commanders.

- The **Dependent Airborne Node** (DAN) enables subordinate commanders that are flying in formation (connected with their leaders operating a KEN) to receive critical situational awareness updates through the intra-aircraft data and voice capability. Through the DAN, commanders can utilize services such as chat and radio voice in order to maintain the lines of communications with their leaders and peers within the same flying formation.

- The **Command And Staff Palletized Airborne Node** (CASPAN) coupled with the KEN provides the Airborne task force commander and his staff with a complete platform to conduct mission planning while enroute to the target area. In addition to EMC's individual workstations, this large roll-on/roll-off workstation is designed for in-flight mission command collaboration.

A | Signaleers from the 270th Signal Company, 50th Expeditionary Signal Battalion-Enhanced provided enroute communication services to joint partners during the 437th Airlift Wing's Mass Generation Exercise 2023, involving 24 C-17s. The 270th Soldiers enabled enroute comms to the Air Mobility Commander and to 2nd Battalion, 10th Marines in support of a fires mission.

B | U.S. Army Sgt. Isaiah Lumar and Spc. Noel Martinez validated connectivity of Army Unified Directory Service devices enroute to North Macedonia. Operators from the 509th Strategic Signal Battalion, provided organic theater Enroute Mission Command (EMC) capabilities to the 173rd Airborne Brigade during Exercise Swift Response May 7 to 11 2024. Both Soldiers are assigned to the 2d Theater Signal Brigade.

C | U.S. Army Capt. Shenelle Stallings provides and Enroute Mission Command capabilities briefing to 173rd Airborne Brigade members before a joint forcible entry operation May 7, 2024, at Aviano Air Base, Italy. The EMC furnishes rapidly deploying tactical units with essential in-flight mission command capabilities and seamless network communications between aircraft and ground forces, which are vital for the success of joint forcible entry operations. Captain Stallings is the commander of the 509th Strategic Signal Battalion's Headquarters and Headquarters Detachment.

HIGH-CAPACITY RADIO SYSTEMS

A

The high-capacity radio technologies in the Product Manager Network Modernization portfolio provide commanders with line-of-sight communication options – as well as beyond-line-of-sight via the current and next generation Tropospheric Scatter Transmission (TROPO) capabilities -- for a more resilient network in congested and contested environments. These high-capacity radio systems address the growing demand for distributing high-bandwidth data in harsh tactical environments, with lower latency than satellite communications (SATCOM). The solutions enable increased data flow between upper and lower echelons, and improved data fusion into the common operational picture at the brigade level and above.

PEO C3N

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

The Arny's high-capacity radio technologies are easy-to-deploy, set-up and tear-down to enable units to relocate rapidly, while delivering resilient network transport to ensure the exchange of critical real-time battlefield situational awareness to keep forces safe and ensure mission success. They improve the expeditionary nature of U.S. Army units, while significantly increasing network throughput and range, operational flexibility and network resiliency through multipath diversity and enhanced primary, alternate, contingency and emergency (PACE) communications plans.

The **Terrestrial Transmission Line-Of-Sight** (TRILOS) Radio is deployed in a few transit cases, and its small form factor provides a significant reduction in size, weight and power (SWaP) compared to the High Capacity Line Of Sight (HCLOS) radio that it replaces. The system is much easier and faster to set up, operate, and maintain. The TRILOS Radio increases the robustness of the Army's tactical network by providing a significant increase in bandwidth and range, with lower latency than SATCOM. TRILOS enables commanders to push smaller units further out to the edge of the battle while keeping them connected to the network. It can also serve as relay capability and transfer signals to distant units.

The Army's new T**ropospheric Scatter Transmission – Medium** (TROPO-M) capability will provide expeditionary beyond-line-of-sight (BLOS) capability without satellites that will extend network range and significantly increase throughput, while greatly reduce SWaP requirements, compared to the current TROPO capability that it will replace. It uses tropospheric scat-

tering capability, which bounces signals off of the Earth's troposphere to provide high-capacity beyond-line-of-sight capability without using expensive and limited satellite resources. It also uses particles in the atmosphere as reflectors for microwave radio signals. The Army began fielding the new TROPO-M in late 4QFY24 to replace the current TROPO system in the field.

The **Line of Sight** (LOS) **Backhaul Radios** are similar to TRILOS but with less range and bandwidth. However, unlike TRILOS, this resilient mesh radio does not use directional antennas; it provides point-to-point, multi-point to point and multi-point to multi-point connectivity. It is portable, rapidly deployable, and units are able to operate on the move.

This brigade and battalion-level mesh radio is an extension of the line-of-sight radio network provided by TRILOS, and it is self-forming/self-healing without need for human intervention. Mesh radio nodes are provided for command post use, integrated onto vehicles (such as Strykers and Joint Light Tactical Vehicles) and can even be used from Unmanned Aircraft like Gray Eagle and variable height antennas.

The **Tactical Radio Integration Kit** (TRIK) provides radio-bridging capability at the battalion and company level. TRIK integrates multiple varieties of tactical radios to enable different user groups, such as U.S. and coalition forces, to seamlessly communicate with different radios. All of the radio technologies are key components of the Army's Capability Set modernization efforts, including the ESB-E and the Integrated Tactical Network (ITN) equipment sets, providing high-capacity terrestrial data transport.

A ǀ 67th Expeditionary Signal Battalion (ESB) new equipment training and fielding for the expeditionary TRILOS Radio.
B-C ǀ Project Manager Tactical Network provides new equipment training and fielding on the modernized Expeditionary Signal Battalion-Enhanced (ESB-E) network communications equipment set – including this TRILOS Radio - to the Maryland U.S. Army Reserve 392nd ESB, 359thTheater Tactical Signal Brigade, 335th Signal Command, at Joint Base McGuire, Dix, Lakehurst (JB MDL), New Jersey, on August 9, 2024
D ǀ Product Manager for Network Modernization (PdM NetMod) held a Troposcatter Transmission-Medium (TROPO-M) Soldier Touch Point (STP) event at Fort Liberty, North Carolina, with the 50th Expeditionary Signal Battalion-Enhanced (ESB-E), in May 2024.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

SECURE WIRELESS

A

The Army's Secure Wireless systems use the National Security Agency (NSA)-approved Commercial Solutions for Classified (CSfC) solution to provide secure classified and unclassified Wi-Fi to the Command Post (CP), with prototype capability also enabling vehicle-to-vehicle wireless communication. Secure Wireless provides agility and operational flexibility, enabling commanders and staff to stay securely connected with full situational awareness and mission command capability for the maximum amount of time possible during CP relocation.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

By going wireless, command post set up and tear down times are significantly reduced, for increased unit maneuverability, operational flexibility, and survivability. Following CP setup, units can turn on their Secure Wireless and the network will come up first instead of last as with cabling, in minutes instead of hours, and Soldiers can stay connected longer when jumping the CP.

The logistical burden is also reduced with less cable and protective flooring needed to be transported from location to location. Soldiers can be untethered from their workstations with wireless laptops for improved collaboration.

Command Post Wireless Small Form Factor (CPW SFF) provides secure wireless capability in the command post and other structures, enabling untethered mission command and data exchange through wireless laptops, tablets, and phones. Project Manager Tactical Network fielded a **Secure Wireless Campus Wide Local Area Network** (CWLAN) upgrade to improve system resiliency, ease of use and reduce setup/tear down times even further, for increased unit mobility and command post survivability.

To improve units' expeditionary command-post capabilities, PEO C3N's Command Post Integrated Infrastructure (CPI2) modernization efforts will provide mobile, scalable and survivable platforms and further increase command post survivability. Secure Wireless is a key component of this effort and is being integrated on prototype vehicles, enabling Soldiers to pull up to any site and connect to the network in minutes. This enhanced system, known as **Secure Wireless Mesh Remote Endpoint** (SWMRE), provides a vehicle-to-vehicle wireless connection that enables units to disperse their command post vehicles, making the command post more survivable.

The **Mobile Broadband Kit** (MBK) is a ruggedized, cloud-managed 3G/4G LTE/5G networking platform designed to provide connectivity across a broad range of network devices. MBK enables all connected devices to push and/or pull both data and position location information to/from the secure cloud via Wi-Fi and cellular. It can be used in a CP or on-the-move for local Wi-Fi bubble without the cellular backhaul enabled.

CAPABILITIES

- Enables an expeditionary CP, significantly reducing CP setup and teardown time; eliminates 17 boxes of expensive cable weighing hundreds of pounds.
- Fast and easy set up / tear down for rapid relocation and maneuver
- Enables commanders and staff to leverage their mission command systems much sooner, resulting in a more accurate and timelier common operating picture, improving military decision process effectiveness and unit survivability.
- Secure Wireless provides agility and operational flexibility, enabling commanders and staff to stay securely connected with full situational awareness and mission command capability for the maximum amount of time possible.
- SIPR without Encryption Hardware: NSA-approved CSfC software-based encryption.
- Transport Agnostic, Multi-Security Enclave Network.
- Works with commercial, NIPR, SIPR, and coalition networks.
- Up to 200 simultaneous laptops connected.

A-B | Soldiers from the 4th Infantry Division use Command Post Integrated Infrastructure (CPI2) capabilities, including SWMRE, during a command post exercise at Fort Carson, Colorado.
C | Project Manager Tactical Network provided new equipment training to Soldiers from the 57th Expeditionary Signal Battalion Enhanced at Fort Hood, Texas.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

CCE & CS-HUB

To support Multi-Domain Operations, the U.S. Army works side-by-side with coalition forces in a Mission Partner Environment, or MPE. In this coalition network environment, data is fluidly exchanged between interoperable systems so forces can contribute to a common operational picture from which commanders can make informed rapid decisions.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

Commercial Coalition Equipment (CCE) is a core component of an MPE. It provides expeditionary coalition or commercial network connectivity to enable mission command, network communications -- voice, video, and data -- and situational awareness between Army, joint and coalition forces. Each of the coalition countries has their own unique transport networks that enable them to connect into the combined coalition network. The U.S. Army uses CCE to connect to the coalition network over its tactical communications network. This easy-to-transport system enables the Army to both send and receive select critical situational awareness with its coalition partners and contribute to a trusted real-time common operating picture across the theater of operations. The CCE can be rapidly reconfigured to provide secure tactical access for the coalition or commercial networks, to support both civil and military operations. .

- **CCEv2**: connects multiple voice networks to radio nets so that key personnel not ordinarily a part of the radio network can join without requiring a radio.

- **CCEv4**: is designed to enable U.S. Army forces to implement MPE interoperability concepts for information exchange and rapid technical integration with NATO and coalition partners. Leveraging an innovative small form factor technology design, the integrated radio-bridging and voice-cross Land and Mobile Radio (LMR) module enables CCEv4 to establish multination radio information exchanges between telephones, combat FMZ networks, and voice applications in support of MPE command and control operations.

- U.S. Army Soldiers and coalition partners use the **Common Services-Hub** (CS-Hub) -- comprised of a CCE variant and the Tactical Server Infrastructure (TSI) -- to host mission partner enterprise services, such as email, Voice over Internet Protocol (VoIP), file sharing, chat and video teleconferencing. The TSI is comprised of ruggedized laptops that function as servers and host a variety of battle command applications.

CAPABILITIES

- Enables voice, video, and data communications and mission command between U.S. and coalition force networks.

- Core components of an interoperable Mission Partner Environment.

- Provides secure tactical access for coalition or commercial networks to support both civil and military operations.

- CCE reduces size, weight and power (SWaP) for initial entry operations and increased unit agility.

- Provides access to commercial internet and phone services through the Tactical Network Regional Hub Nodes.

- Enables mission partner enterprise services, such as email, VoiP, file sharing, chat and video teleconferencing.

A | Maj. Ryan Hamilton, a field artillery officer with the 1st Cavalry Division Artillery, works alongside Polish officers during Avenger Triad 24, Sept. 11, 2024, in Boleslawiec, Poland. Avenger Triad 24 is a U.S. Army Europe and Africa command post exercise with U.S. Army, NATO and multinational organizations occurring 9-19 September 2024, in multiple locations in Europe. Incorporating lessons learned from Austere Challenge 24, this exercise implements operational concepts, doctrine and procedures to increase readiness, enhance interoperability, employ new concepts, and inform regional planning.
B | PdM NetMod provided CCEv4A new equipment training and fielding for the 30th ESB-E, 11th Airborne Division in Anchorage, Alaska, in April.

B

MCN-AE

Sharing intelligence data is critical to successful missions on the battlefield. The small form factor Modular Communications Node-Advanced Enclave (MCN-AE) augments the existing intelligence network, enabling intelligence users to connect to all the same resources they have when using the traditional standalone TROJAN Intelligence Network, but instead using the Army's Tactical Network.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

Each MCN-AE fits into a suitcase-sized transit case, and the system uses a unit's organic tactical network transport equipment to relay intelligence data across the battlefield. MCN-AE enables the Army to replace the tactical elements of the intelligence network's TROJAN Special Purpose Integrated Remote Intelligence Terminal (SPIRIT) system, a large truck and trailer, with two carry-on cases, cutting down on footprint. The system reduces size, weight and power (SWaP) requirements for a more expeditionary force while increasing a unit's operational flexibility.

MCN-AE improves operational flexibility and multipath diversity. Unlike the current TROJAN Network that only uses the TROJAN SPIRIT system for network transport, the Tactical Network provides numerous network transport options via a wide range of Army transport nodes. These network transport nodes can operate in all satellite bands (Ka, Ku, X-band, etc).

The MCN-AE also enables commanders conducting operational missions to dynamically assign bandwidth between their tactical mission command and intelligence assets as they see fit, with the ability to reassign additional bandwidth on demand.

Traditionally, in the past, the Army's tactical operations, intelligence, logistics and medical communities each used separate communications networks to pass information. The Army is converging the intelligence, logistics and portions of the medical networks onto the tactical network, an effort, known as Transport Convergence. The lightweight expeditionary MCN-AE is at the heart of the intelligence convergence effort – Phase 1 of Transport Convergence.

CAPABILITIES

- Provides intelligence data exchange with commercial off-the-shelf or government off-the-shelf baseband network

- Reduces SWaP for increased unit agility

- Enables commanders conducting operational missions to dynamically assign bandwidth between tactical mission command and intelligence assets, with the ability to reassign additional bandwidth on demand

- Uses the robust and redundant tactical network, delivering needed redundancy to the intelligence community

A | The small form factor MCN- AE augments the existing intelligence network, enabling intelligence users to connect to all of the same resources they have when using the traditional TROJAN Intelligence Network, but instead using the Army's Tactical Network.

B | Each MCN-AE fits into a suitcase-sized case, and the system uses a unit's organic tactical network transport equipment to relay intelligence data across the battlefield.

C | PM Tactical Network demonstrated MCN-AE to Army leadership at the Army National Guard G6 Mission Command Workshop at Little Rock, Arkansas.

SATCOM FAMILY OF TERMINALS

The Army's flexible, modular, scalable and tailorable Satellite Communication (SATCOM) Family of Terminals (FoT) provide an optimal variety of expeditionary, mobile satellite terminals to units worldwide to best support different formations, echelons, mission requirements and locations. These SATCOM systems provide global voice and data network communications, and the exchange of time-sensitive situational awareness, intelligence, and mission command information, while at-the-quick-halt, during all operational phases, echelons and missions. The commercial Family of SATCOM Terminals supports Command Post mobility and survivability by providing several easy-to-deploy, quick-set up/tear down communications solutions to enable units to relocate rapidly, while delivering critical real-time battlefield situational awareness to keep forces safe and ensure mission success.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

In support of the Army's network goals to support Large Scale Combat Operations, the service is leveraging the Family of Terminals acquisition strategy to support its expeditionary SATCOM needs. This strategy allows for procurement of the most capable and formation appropriate terminals to best suit requirements. The Army plans to further consolidate the current variety of ground satellite equipment in its portfolio, leveraging the more versatile "family of systems" approach, while retaining the acquisition flexibility to insert new technologies as they evolve.

The Army's future SATCOM portfolio is expected to include emerging commercial high-throughput, low latency (HT/LL) network transport, such as Low Earth Orbit (LEO) and Medium Earth Orbit (MEO) and advanced high-throughput Geosynchronous Earth Orbit (GEO) SATCOM. One solution currently in development, the Next Generation Tactical Terminal (NGTT), will simultaneously leverage emerging HT/LL LEO and MEO constellation providers and current and future GEO constellations, as well as multiple frequency bands, with a single terminal.

FY 2025 SYSTEMS

Currently, PdM SATCOM manages a Suite of SATCOM Terminals (SoT) within the Army's larger FoT portfolio.

- Extra Small:
  SoT - Global Rapid Response Information Package (GRRIP) and modernized **T2C2-Ultra Lite**: [Integrated antenna] - Fits into a single handheld airline carry-on transit case for rapid mobility and force scalability; sets up and connects in minutes; utilizes L-Band; supports multiple security and mission enclaves

- Small:
  SoT - SCOUT-Small (0.65m/0.95m): Transportable in three hard side transit cases; supports 12 users over multiple enclaves, airline checkable for commercial transport; rapidly setup by two Soldiers; tri-band capable (X, Ku, & Ka)

- Medium:
  SoT - SCOUT-Medium (1.3M): Transportable in four hard side transit cases; supports 48 users over two enclaves; airline checkable for commercial transport; rapidly setup by two Soldiers; tri-band capable (X, Ku, & Ka).
  - **Scalable Network Node**- See TNT-ATH
  - **Sustainment Transport System SATCOM**- See STS

- Large:
  SoT - T2C2 Heavy (2.4m ISA): Transportable in seven hard side transit cases; supports 48 users over multiple enclaves; airline checkable for rapid commercial transport; quick setup by two Soldiers; tri-band capable (X, Ku, & Ka); used by brigades, divisions and corps
  - In the future, FoT-Large will support the **Large Deployable Terminal (LDT)** that will replace the current **Satellite Transportable Terminal (STT)** (managed by PdM Mission Network).
  - In the future, FoT-Large will also support the **Phoenix Terminal Program**.

- Extra Large:
  The **Extra Large Deployable Terminal (XLDT)** will replace the current **Tactical Hub Node** (TCN) managed by PdM Mission Network, with the next generation enhanced THN to be known as
  - **Deployable Ku/Ka/X-band Earth Terminals** (DKETs) also serve as one of the extra-large terminals in the Family of SATCOM Terminals portfolio.

A-B ǀ A Soldier from the 2nd Security Force Assistance Brigade (2nd SFAB) configures a SCOUT satellite terminal to increase tactical communication to support exercise African Lion 2024 (AL24) in Dodji, Senegal, May 27, 2024.
C ǀ Soldiers with the 3rd Brigade Combat Team, 101st Airborne Division (Air Assault) operate a Scalable Class Of Unified Terminals (SCOUT) during the unit's Integrated Tactical Network validation exercise, where they operated the full ITN suite to communicate from dismounted operations up to the command post headquarters.

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

PHOENIX

The new Phoenix E-Model, which replaces the larger footprint D-Model, is being fielded to Expeditionary Signal Battalion-Enhanced (ESB-Es) and other critical formations to provide large division and corps headquarters with agile high-bandwidth network communications. Phoenix terminals provide high capacity, inter- and intra-theater range extension. They are used for high-throughput missions, which include Unmanned Aerial System feeds, video teleconferencing, and large numbers of subscribers and computers on the network.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

These versatile transportable, quad-band, satellite terminals enable operational flexibility and multipath diversity, by providing a rapidly deployable capability that can operate over military X/Ka and commercial C/Ku satellite bands. They also support point-to-point, mesh, and hub-spoke networks.

The new Phoenix E-Model serves as the largest satellite capability for the Army's new ESB-E formations, in addition to the units' small and medium ground satellite terminals.

Like the current Phoenix D-Model, the flexible Phoenix E-Model prototype operates on four different satellite bands (military X/Ka and commercial C/Ku-bands), however, its dual-head capability enables the use of two antennas on two different frequency bands, or two different satellites, simultaneously. This reduces manning requirements for equivalent capability, doubles bandwidth throughput, and enhances multipath diversity and resiliency within the tactical network. In addition to operating on traditional Geosynchronous Earth Orbit (GEO) satellites, the Army is assessing the potential to leverage Phoenix E-Model to operate on evolving Medium Earth Orbit (MEO) constellations.

The current Phoenix D-Model is completely vehicle-based, with a permanent vehicle-mounted antenna. Contrarily, the new E-Model is transit case-based, which enables Soldiers to remove the equipment from the vehicle so they can easily deploy and operate the system without the vehicle, increasing the unit's expeditionary nature, mobility and operational flexibility in support of a variety of missions around the world.

CAPABILITIES

- Operates on four different satellite bands (military X/Ka and commercial C/Ku-bands) for operational flexibility and multipath diversity.

- Supports point-to-point, mesh, and hub-spoke networks.

- Phoenix E-Model dual-head capability enables the use of two antennas on two different frequency bands, or two different satellites, simultaneously. This reduces manning requirements for equivalent capability, doubles bandwidth throughput, and enhances multipath diversity and resiliency within the tactical network.

- Transit case-based capability is easier to deploy; system can operate without the vehicle

- Potential to leverage Phoenix E-Model to operate on evolving Medium Earth Orbit (MEO) constellations.

A | The 2nd BCT, 1st ID used this SMART-T at Hohenfels Training Area, Germany during Allied Spirit VIII.
B | Project Manager Tactical Network provided Phoenix E-Model satellite terminal training to the 57th Expeditionary Signal Battalion-Enhanced (ESB-E), 11th Corps Signal Brigade, at Fort Cavasos, Texas, in December 2023.
C | PM Tactical Network conducts Phoenix E-Model new equipment training to the 51st ESB-E at Joint Base Lewis McChord, Washington in January 2024.
D | PM Tactical Network conducts Phoenix-E Model new equipment training for the 44th Expeditionary Signal Battalion-Enhanced, 2d Theater Signal Brigade, in August 2024

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

SMART-T

A

The Secure, Mobile, Anti-Jam, Reliable, Tactical Terminal (SMART-T) is a protected satellite terminal that provides resilient global beyond-line-of-sight (satellite) data exchange for the current and future unified network. The system enables commanders at brigade and higher to operate in an electronic warfare threat environment that includes both radio frequency signal interference (jamming), signal detection and geographic location threats. SMART-T makes it possible for units to reliably and securely extend the range of their network in such a manner that communications cannot be jammed, detected or intercepted, enabling Soldiers to send critical text, data, voice and video communications beyond their area of operations.

PEO C3N

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

Additionally, the SMART-T can also survive the effects of a high-altitude electromagnetic pulse produced by nuclear detonations and can operate and survive in a biological and chemical environment.

SMART-T uses the Advanced Extremely High Frequency (AEHF) satellite constellation, providing the Army with the highest level of protected communications. Additionally, SMART-T provides fully interoperable communications with the AEHF and Milstar terminals of other services (US Air Force, US Navy, US Marine Corps, and other DoD agencies and activities).

CAPABILITIES

- Interoperable with AEHF satellite constellation

- Enhanced system interfaces

- Provides anti-jam and anti-scintillation (nuclear environment) communications

- Provides Low and Medium Data Rate or Extreme Data Rate capability for voice and data transmission via Serial and/or IP interfaces

- New Case, Electronic Communications Equipment Serial to IP conversion capability

A ׀ **The 2nd BCT, 1st ID used this SMART-T at Hohenfels Training Area, Germany during Allied Spirit VIII.**
B-C ׀ **Members of Charlie Company, 44th Expeditionary Signal Battalion-Enhanced, 2d Theater Signal Brigade, conduct field communications and data tests between the Terrestrial Transmission line of sight radio systems via the SMART-T near Baumholder, Germany.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

DKET

A

Deployable Ku-band Earth Terminals (DKETs) are commercial non-program of record satellite systems that are designed for use at larger hub locations – such as brigade and higher headquarters elements -- to augment the Army's unified tactical communications network infrastructure. The versatile DKET can operate on commercial Ku-, Ka and X-band. They are transportable and self-contained, and can establish headquarters-level, network-hub connectivity anywhere a mission dictates.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

Some of the DKETs take on dual roles as hubs, providing inter- and intra- theater satellite links at brigade and higher, and linking multiple regional command headquarters. DKETs reduce network traffic load on the Army's five global Regional Hub Nodes by providing network hub services for disadvantaged forward units. They also come in a vehicle-based version, known as a Mobile DKET, or MKET).

DKETs also support other countries, services and agencies world-wide. This support is expanding to include DKETs in fixed locations, the Fixed DKET, or FKET.

The Army's new Satellite Communications (SATCOM) Terminal Remote Monitor Management Network (STRMM) enables management and control of a DKET from a secure remote location, helping to reduce Field Service Representative footprint.

CAPABILITIES

- Three configurations: DKET Light (3.7 – 3.9M), Mobile DKET (4.5M) and Standard DKET (4.6M – 7M), with the majority being the light design

- Establishes headquarters-level, network-hub connectivity anywhere a mission dictates

- DKETs operate on Ku, Ka and X-band frequencies

- DKET Light has a tri-fold antenna and a smaller shelter to make redeployment and setup faster and easier

- The robust DKET network makes for a seamless transition to backup equipment or terminals, eliminates long outages and minimizes impact to the Soldier

- Transportable and self-contained; electronics housed in separate shelters

- Reduces network traffic load on the Regional Hub Nodes by providing network hub services for disadvantaged forward units

A ı **A DKET is shown as part of Project Manager Tactical Network's Ka and X-band frequency certification effort that enables earth satellite terminals to utilize military satellites.**
B ı **DKETs support commercial Ku-Band frequencies and their electronics are housed in separate shelters. They are highly transportable, self-contained and can establish headquarters-level, network-hub connectivity anywhere a mission demands.**
B ı **DKETs also come in a vehicle-based version, known as a Mobile DKET, or MKET.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

STS

A

Sustainment Transport System (STS) provides secure, expeditionary, easy to use, global data transfer for the logistics community -- including logistics, personnel, medical and force protection data -- to enable the rapid delivery of the right supplies and personnel to the right locations on the battlefield. Developed for the general purpose user, these easy to deploy network transport systems will provide the resilient, high-capacity connectivity needed to enable the exchange of critical logistics information worldwide.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

The U.S. Army continues to modernize the way it exchanges logistics data, both globally and locally on the battlefield. In support, in fiscal year 2023 the service established three new STS data transport programs of record (PoRs): STS Satellite Communications (SATCOM), STS Line-of-Sight, and STS Wireless-Fidelity (Wi-Fi).

The legacy logistics network program, known as the Combat Service Support (CSS) network, has been in operation since 2004. PdM UNCI continues to deliver bridge enhancements across the Army's current fleet of logistics systems to make the CSS network more secure and capable. PdM UNCI will continue to manage CSS systems until the STS network systems are fielded across the force.

To support STS SATCOM, commercial ground satellite terminals provide the tactical network transport needed to enable global data exchange for the Army's logistics information systems and applications, such as Enterprise Resource Planning (ERP), Global Combat Support System-Army (GCSS-Army), Integrated Personnel and Pay System-Army (IPPS-A), Medical Communication for Combat Casualty Care (MC4) and General Fund Enterprise Business Systems (GFEBS). Th new STS SATCOM systems expand current CSS SATCOM capabilities to operate on both commercial and military satellites on Ku, Ka, and X bands.

For local data exchange across battlefield logistics support locations, STS Line-of-Sight increases the range and speed of existing line-of-sight data transmission solutions, while STS Wi-Fi provides secure wireless connectivity at each of the STS network nodes. All of the easy-to-use STS expeditionary network transport systems are developed for general-purpose users and can be rapidly setup and torn down for enhanced unit maneuverability.

The modernized STS solutions also provide a more robust capability to support predictive maintenance, telehealth services, and other emerging sustainment services that support the Warfighter.

CAPABILITIES

- Secure high-capacity global tactical network transport – SATCOM, Line-Of-Sight and Wi-Fi

- Fully capable to integrate into the Army's unified network

- Leverages the Regional Hub Nodes and Global Agile Integrated Transport

- Commercial auto-acquire satellite terminals

- Easy to use for general purpose user

- Easy to transport for rapid deployment and battlefield mobility

- Supports Army Enterprise Resource Planning solutions

A � Project Manager Tactical Network facilitated a STS risk reduction event (RRE) assessment, at Electronic Proving Ground, Fort Huachuca, Arizona, in September 2024, to reduce risk for the STS Initial Operational Test in fiscal year 2025. STS Satellite Communications (SATCOM) seen here during the event.
B ۀ Project Manager Tactical Network facilitated a STS RRE assessment, at Electronic Proving Ground, Fort Huachuca, Arizona, in September 2024, to reduce risk for the STS Initial Operational Test in fiscal year 2025. STS Line Of Sight seen here during the event.
C-D ۀ Project Manager Tactical Network conducted a Soldier touch point validation event in August 2024 to ensure the accuracy of the technical manuals (TMs) for all three STS programs of record -- STS SATCOM, STS Line Of Sight and STS Wi-Fi (seen here).

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

| UNIFIED NETWORK | COMMON OPERATING ENVIRONMENT | JOINT & COALITION INTEROPERABILITY | CP MOBILITY/SURVIVABILITY |

AIT

Product Lead Allied Information Technology (PdL AIT) provides non-standard, Information Systems (INFOSYS), Enterprise Resource Planning, Cybersecurity, and C5I (Command, Control, Communications, Computers, Collaboration, and Intelligence) solutions to build resilient and interoperable forces for U.S. Allies and Partner Nations through the Foreign Military Sales (FMS) process. PdL AIT products are unique systems based on Commercial-Off-The-Shelf (COTS) technologies and customized to meet partner nation requirements.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

ONE NETWORK
PROJECT MANAGER
TACTICAL NETWORK

DESCRIPTION

AIT solutions are tailored according to host nation requirement and coalition standards (e.g., NATO), enabling foreign partners to better secure and defend their individual sovereignty and increasing their capacity for contribution to the broader collective security posture. AIT's work supports mutual U.S. and allied interests by strengthening bilateral defense partnerships, enhancing coalition building through interoperability, and increasing the readiness of our partners in uncertain, complex and potentially hostile security environments.

CAPABILITIES

- PdL AIT products are unique systems based on Commercial-Off-The-Shelf (COTS) technologies and customized to meet partner nation requirements.
- Hardware / Infrastructure:
- IT Network Infrastructure Upgrades
- Network Modernization, Hardening, and/or Replacement
- Data Fusion Centers, Security Operations Centers (SOC), Intelligence Centers
- Intelligence Surveillance and Reconnaissance (ISR)
- Future Mission Network (FMN) compliant networks
- Maritime, Air, and Land integration centers
- Continuity of Operations (COOP) sites
- Data / Software:
- Command and Control (C2) Systems
- Disaster Recovery Solutions
- Big Data / Cloud Computing
- Open-Source Intelligence (OSINT) Data Platforms
- Data/Software Commercial Training
- Enterprise Information Systems:
- Pay Systems and Human Resource Management Systems
- Logistics Automation and Supply Chain Information Management Systems
- Medical/Health Records Data Management Systems
- Health Information Systems (HIS)
- Aviation Asset Management Systems
- Security and Cyber Security:
- Defensive Cybersecurity
- Cyber Security Incident Response
- Cyber Virtual Training and Education Environments (Cyber Ranges)
- Cyber Security Operations Centers (CSOC)
- Security Information and Event Management (SIEM), Security Orchestration and Response (SOAR), Extended Detection and Response (XDR) Endpoint Security
- Behavioral Analytics
- Cyber Fly-Away Kits
- Multi-Factor Authentication (MFA) Systems
- Border Security Sensor infrastructure
- Embedded Technical Advisors:
- Cyber, Network, Security, IT, Enterprise Information Systems, Data, software, and additional C5ISR Embedded Technical Advisors
- Commercial Training:
- Security / Cyber Security
- Enterprise Information Systems
- Hardware / Software

A ׀ **PdL AIT products are unique systems based on commercial technologies and customized to meet partner nation requirements.**

COMSEC

Product Manager Communications Security (COMSEC) develops, procures, fields, and sustains the Army and Joint Services' cryptographic mission. Devices within the portfolio receive, store, generate, manage, and distribute National Security Agency (NSA) Cryptographic Key Material across both the enterprise and tactical environment, securing voice and data networks to the TOP SECRET level across the globe.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

COMSEC focus areas include Army Key Management Infrastructure (AKMI) and COMSEC Cryptographic Solutions (CCS). AKMI provides users with an organic key generation capability and a secure, electronic key distribution means to load NSA-generated keys into End Crypto Units (ECUs). AKMI consists of Management Client (MGC), Automated Communications Engineering Software (ACES), Next Generation Load Device (NGLD) family, and Simple Key Loader (SKL).

PdM COMSEC is developing the Next Generation Load Device-Medium (NGLD-M), which will replace the SKL and fulfils COMSEC modernization for key loading across the DoD. The NGLD-M will support stronger cryptographic keys and a more secure method of delivery than the current SKL. These cryptographic key fill devices enable a Soldier to communicate by secure phones, classified computers, and secure VTCs at SECRET, TOP SECRET and other high classification levels. PdM COMSEC also develops CCS, which defends all echelons of the Army Network with modern cipher algorithms.

CAPABILITIES

- **Cryptographic Mission Planner:** Provides ACES crypto network planning; generates Signal Operating Instructions; creates COMSEC key tags.

- **COMSEC Load Devices:** NGLD-Small, SKL and in the future NGLD-M transfer mission critical cryptographic keys fill into ECU devices and tactical radios.

- **Secure High Assurance Inline Encryption (INE) Link Device:** COMSEC Cryptographic Systems are comprised of INEs, which secure the Army's data and voice communication networks. INE encryption devices include inline network and inline media, link and trunk, secure voice, and commercial solutions for classified communications.

A I **2nd Squad assembles and loads Communication Security (COMSEC) into a tactical handheld radio using a Simple Key Loader (SKL) on Aug. 15, 2024, at Fort Leonard Wood, Missouri.**
B I **The NGLD-M will replace aging Simple Loader fill devices and will be used to transfer the strongest NSA-generated cryptographic keys to tactical, strategic, and enterprise network systems.**
C I **Tactical Key Loader (TKL), crypto key device NGLD-S, provides critical command and control of emergency, time sensitive and secure communications during Special Forces missions. The TKL's smaller and dimmer screen reduces detection during nighttime operations, making it a critical capability for U.S. Army special operations.**

HAMMR

A

Helicopter and Multi-Mission Radios (HAMMR) procures tactical communication enhancement equipment, ancillaries, and related services in support of the Army's Unified Network Plan.

PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

HAMMR provides air-ground interoperability between maneuver ground forces and aviation and is the Army's program for the Integrated Tactical Network (ITN) concept tactical radio Commercial Off the Shelf (COTS) procurement, fielding, and sustainment. HAMMR radio products include all Army Link-16 radios (Ground ADA, Ground Fires, Aviation, and Gateways).

High Frequency (HF) **Radios:**

- The modernized PRC-160 is the Army's current beyond-line-of-sight software-defined HF radio supporting the Army's Class II Engineering Change Proposal for ground-based HF requirements to replace the Army's legacy and obsolete PRC-150 HF ground-based radio.

- The PRC-160 meets new NSA crypto-modernization standards, transmits data 10 times faster than the legacy HF radio and is the smallest, lightest and fastest HF Manpack radio systems available.

- The PRC-160 delivers assured and secure communication solutions at the tactical edge and SATCOM-Denied environments through resilient wideband data rates up to 120 kbps.

Air to Ground Networking Radio (AGNR): AGNR uses Program of Record ground radios and a federated integration approach that will allow aviation to keep pace with technological changes on the ground by FY27.

- ANGR maintains air-ground interoperability between maneuver ground forces and Aviation. AGNR will provide commanders enhanced situational awareness and Mission Command to provide a more responsive means of directing aircraft to match changing maneuver forces.

Multifunctional Information Distribution Systems (MIDS):- MIDS Low Volume Terminal (LVT) (2/11) is the DoD's primary Link 16 tactical data link network, which provides interoperability, situational awareness and support for air and missile defense operations at division through corps.

- MIDS Joint Tactical Radio System (Ground Variant) builds upon and will ultimately displace MIDS LVT with a software defined radio solution that introduces modernized Link16 networking.

Next Generation Survival Radio (NGSR): NGSR replaces the current CSEL radio capabilities with a smaller, handheld form factor that meets current cryptographic modernization efforts, enhanced user functionality, and increased survivability.

Rotary Wing Contingency Communications (RWCC): RWCC provides a COTS SATCOM/Cellular Internet communications capability for rotary wing aircraft enabling accredited fly-away kits to conduct Voice Over Internet Protocol (VOIP) calls up to the TS/SCI level.

C5ISR Modular Open Suite of Standards Mounted Form Factor (CMFF) **Radio Cards**: CMFF is the Army's effort to more easily and rapidly equip ground vehicles and aviation platforms with warfighting capability cards plugged into a common chassis to reduce space and increase performance.

- Will leverage analog and digital radio heads to provide radio front ends and antennas, typically mounted on the vehicle's exterior.

- Future designs will address Communications Security (COMSEC) and Transmission Security (TRANSEC) requirements of various waveforms with the Cryptographic Subsystem (CSS) card.

A | The HAMMR portfolio provides units such as the 101st Airborne Division (Air Assault) with modernized radio variants that provide secure communications from the air down to the tactical edge.

B | C5ISR/Electronic Warfare (C5ISR/EW) Modular Open Suite of Standards (CMOSS) Mounted Form Factor (CMFF) in Figure 1 illustrates the CMFF components.

C | Soldiers from the 30th Signal Battalion conducted a radio check during a tactical radio competition during Signal Week at Schofield Barracks, Hawaii, Feb. 27, 2024. High Frequency (HF) radios continue to provide Soldiers with long-distance communications across the world to enhance Indo-Pacific readiness.
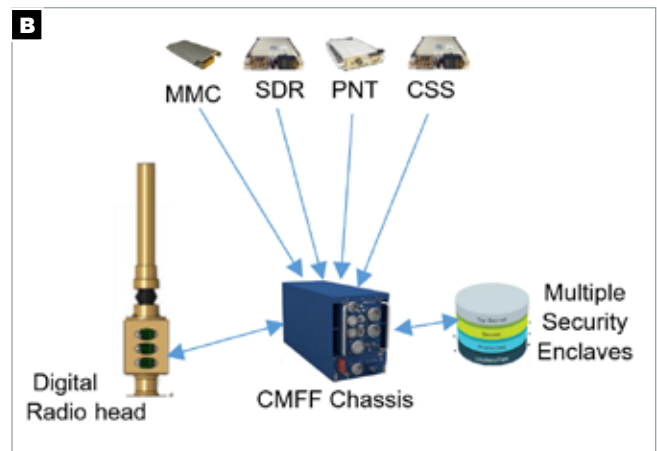
HMS

Handheld, Manpack and Small Form Fit (HMS) acquires Non-Developmental (NDI) radio solutions, providing affordable networking tactical radio systems that meet operational requirements from the Army. Other customers include the Marine Corps, Navy, and Special Operations Command (SOCOM). HMS products provide state-of-art networking waveforms, provide human factor upgrades over legacy radio solutions, and are interoperable with specified radios within the current force.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

HMS is the total lifecycle manager for tactical radio communication. Paramount to the HMS mission is providing interoperable communications to the tactical edge Warfighter with an on-the-move, at-the-halt and stationary Line of Sight (LOS)/Beyond the Line of Sight (BLOS) capability for both dismounted personnel and platforms. HMS radios provide voice communications as well as support for data services such as text, control graphics, imagery, and video to the tactical edge Warfighter through interoperability with tactical End User Devices (EUDs), and provide Single Channel Data Radios (SCDR), primarily in support of the Integrated Visual Augmentation System (IVAS). HMS products enable net-centric operations, operate in multiple bands and multiple modes, and deliver reliable, secure tactical communications. They are network-scalable to meet operational needs and are developed based on reprogrammable modular Software Communications Architecture (SCA), allowing field and depot service to upgrade such features as security and waveforms.

Full Rate Production (FRP) Leader Radio:

- AN/PRC-148C, Two-Channel, Channel 1: Single Channel Ground Airborne Radio System (SINCGARS), Channel 2: Tactical Scalable MANET (Mobile Ad Hoc Networking) (TSM)™

- AN/PRC-148D, Two-Channel, Channel 1: SINCGARS, Channel 2: Warrior Robust Enhanced Network (WREN) TSM, WREN Narrowband (NB)

- AN/PRC-148F, Two-Channel, Channel 1: SINCGARS, Channel 2: WREN TSM, WREN NB

- AN/PRC-163, Two-Channel, Channel 1: SINCGARS, Channel 2: WREN TSM, WREN NB

FRP Generation 2 Manpack Radio:

- AN/PRC-158, Two-Channel, Type 1 and Type 2, Saturn, MUOS, SINCGARS, SATCOM, WREN TSM™, Full Rate Production (FRP).

- AN/PRC-162, Two-Channel, Type 1 and Type 2, Saturn, MUOS, SINCGARS, SATCOM, WREN TSM™, Full Rate Production (FRP).

Single Channel Data Radios (SCDR):

Single Channel data only radio; Provides data exchange between Integrated Visual Augmentation System (IVAS) users; Operates on Sensitive But Unclassified - Encrypted (SBU-E)

- SM4210-235-5B - Single Channel, MN-MIMO Waveform

Single-Channel Assured Voice and data Radios (SCAR):

Single Channel voice and data radio; Operates on Sensitive But Unclassified - Encrypted (SBU-E) only

- AN/PRC-166 - Single Channel, TSM

- AN/PRC-168 - Single Channel, TSMs

- AN/PRC-170 - Single Channel, TSM

- AN/PRC-171 - Single Channel, TSM

A ı Operational exercises such as the annual Super Garuda Shield with the 25th Infantry Division in Indonesia provide an opportunity for Soldiers to experiment with multiple HMS radio variants in an operational environment.
B ı U.S. Army Soldiers, Spc. Benjamin Hernandez (left), and Pfc. Keeshawn Johnson, conducts a functions check on a MUOS Manpack Radio during Joint Multinational Readiness Center, Wahiawa, Hawaii, Oct. 3, 2024.
C ı Single Channel Data Radios provide Soldiers with the ability to transmit voice, data and video in a SBU-E network environment, which provides network resiliency without the complexity of setting up a network for easier communications among team and squad leaders and more streamlined coalition partner sharing as seen here during the annual Super Garuda Shield Indo-Pacific exercise with the 25th Infantry Division in September 2023.

ITN

The Integrated Tactical Network (ITN) is delivering a tactical network that is providing expeditionary, mobile, simple to use and hardened capabilities – now from air-to-ground and division-to-edge – for enhanced situational awareness and seamless command and control.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

As a critical component to the Army's Unified Network Plan, the ITN continues to revolutionize the way commanders and Soldiers communicate. The ITN incorporates the Army's current tactical network environment (applications, devices, gateways, and network transport) with commercial off-the-shelf components and transport capabilities.

ITN technologies enable communications through a Sensitive but Unclassified-Encrypted (SBU-E) enclave for a network that is more secure and resilient by offering units multiple network communication pathways when faced with contested or congested communications environments. Since the majority of tactical information below the battalion level is perishable in nature and unclassified, the SBU-E addresses the need to cut the line between having a secret, Type 1 encrypted network to a network that is still encrypted and safe.

The SBU-E also allows for better mission partner interoperability, which is a critical capability because the Army will never fight alone.

As the Army adapts and evolves its network to reduce complexity and tailor capabilities at echelon, the ITN's flexibility is allowing higher echelons to take on complex network planning and management, while retaining necessary network capabilities for commanders at lower echelons who are focusing on the fight.

The 82nd Airborne Division, 25th Infantry Division, and 101st Airborne Division, Air Assault, have successfully incorporated the ITN at their division echelons.

As part of the Army's experimental modernization concept, called "transformation in contact," the 2nd Brigade Combat Team, 101st Airborne Division (Air Assault) (2-101) conducted Large-Scale, Long-Range Air Assault exercises to help the Army refine the new ITN Aerial Toolkit. The kit incorporates a radio in the crew compartment serving as the communications node connecting a Tactical Assault Kit (TAK)-enabled tablet to dismounted Soldiers, to enable shared chat and position location information over SBU-E.

With the addition of Mobile User Objective Systems (MUOS) Manpack satellite communications radios to select aircraft, pilots and commanders added beyond line-of-sight voice and data capability to their arsenal.

Fielding the ITN at the division echelon was made possible following six years of iterative DEVOPS and fielding to 11 brigade combat teams, six security force assistance brigades, and several division enablers. The Army will continue to field and iterate the ITN across the force for the foreseeable future.

A I **Soldiers with the 101st Airborne (Air Assault) conducted multiple Large-Scale, Long-Range (L2A2) exercises throughout 2024 using the ITN's flexible communications capabilities, including during Operation Lethal Eagle in April, 2024 at Fort Campbell, KY.**
B I **Soldiers with the 1st Battalion, 29th Infantry Regiment (1-29) conduct an Operational User Assessment (when/where) using the ITN to communicate over a Leader Radio connected to a Nett Warrior End User Devise to consolidate the air, ground and fires pictures onto a single common operating picture.**
C I **The ITN's Aerial Toolkit incorporated radios into the cockpit to serve as the communications node that when connected to a TAK-enabled tablet provided air to ground communications over SBU-E between the commander in the air and dismounted Soldiers.**

ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

WAVEFORMS

Product Manager Waveforms provides the warfighter with a suite of scalable and interoperable tactical waveforms and software products, enabling secure tactical communications, seamless networking, and real-time network management capabilities supporting the Army tactical radio portfolio.

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

DESCRIPTION

Product Manager Waveforms provides the warfighter with a suite of scalable and interoperable tactical waveforms and software products, enabling secure tactical communications, seamless networking, and real-time network management capabilities supporting the Army tactical radio portfolio.

CAPABILITIES

CNR:

- The CNR program is part of the SINCGARS modernization strategy that supports National Security Agency and Department of Defense cryptographic modernization goals by providing assured command and control voice, and limited Fires and Air Defense data in environments where access to the ITN is degraded, enabling multiple communications options for commanders.
- The CNR is replacing the RT-1523 series legacy radios. It will also continue to support the modernized SINCGARS waveform and its associated future upgrades.
- The CNR team conducted Field-based First Article Tests at the Electronic Proving Grounds, AZ from August to September. National Guard Soldiers participated in the effort and provided valuable user feedback, noting the CNRs simplicity and enhanced voice clarity and resilience of the modernized Frequency Hopping 3 (FH3) mode.
- An Operational Unit Assessment was completed at Fort Moore, GA during the month of October. The event was facilitated by the Maneuver Battle Lab and put the CNR in the hands-of Soldiers while going through various battle scenarios.

SINCGARS:

- SINCGARS waveform is currently under a modernization effort as part of the NSA DoD Cryptographic Modernization Effort. It provides warfighting commanders and troops with a highly reliable and secure voice and data handling capability in support of Command-and-Control Operations.
- The new SINCGARS waveform will include faster frequency hopping capabilities (FH2 and FH3) for use in mounted vehicle radios and the portable Manpack radio to securely transmit data in contested environments.
- The waveform will be integrated in ground and aviation platforms including the HMS PRC-158 and PRC-162 MP; PRC 148 and PRC 163 LR, RT-1523 series, PRC-152 series, PRC-117 series, Air-Ground Networking Radio and the CNR.

WREN:

- WREN waveform network scalability, increases communication range, reduces spectral footprint, and provides hardened Electronic Warfare protection.
- Supports VHF, UHF and L-Band frequency ranges using 50 kHz,1.2 MHz, 3.6 MHz, and 10MHz+ Bandwidth.
- Provides simultaneous Position Location Information and voice services.
- Operates in two modes to address the Army's existing and future Integrated Tactical Network networking challenges: WREN TSM – provides Spectrum Supportability, Point to point and WREN-NB – provides enhanced Electronic Protection and Spectrum Supportability for operations in contested and congested environments.
- Adopts TSM Barrage Relay networking for extended range and fast frequency hopping.
- WREN supports Type 1 Secret and Below and Sensitive But Unclassified-Encrypted security level interoperability.

enterprise Over The Air Management (eOTAM):

- eOTAM is an Application Programming Interface framework and radio service that simplifies network management and enables secure over the air monitoring and remote re-provisioning.
- Features a standardized and secure protocol defined by the government to provide the ability to manage and monitor the Army's tactical radios securely and remotely.

A-B | The Combat Net Radio Operational User Assessment (OUA) on October 9 and 10, 2024 at the Maneuver Battle Lab, Fort Moore, GA, provided Soldiers with the most comprehensive exercise to date using the new single-channel radio replacement to SINCGARS. This simple to operate radio provided clearer voice transmissions and a resilient modernized Frequency Hopping 3 (FH3) mode than its predecessor in an operational setting with dense foliage and varying elevations.

C | Soldiers with the 2nd Battalion, 501st Parachute Infantry Regiment, assigned to the 1st Brigade Combat Team, 82nd Airborne Division evaluate the AN/PRC-148C Leader radio and the AN/PRC-148D using the Warrior Robust Enhanced Network TSM waveformprotection, and supports anti-jamming and low probability of intercept capabilities.
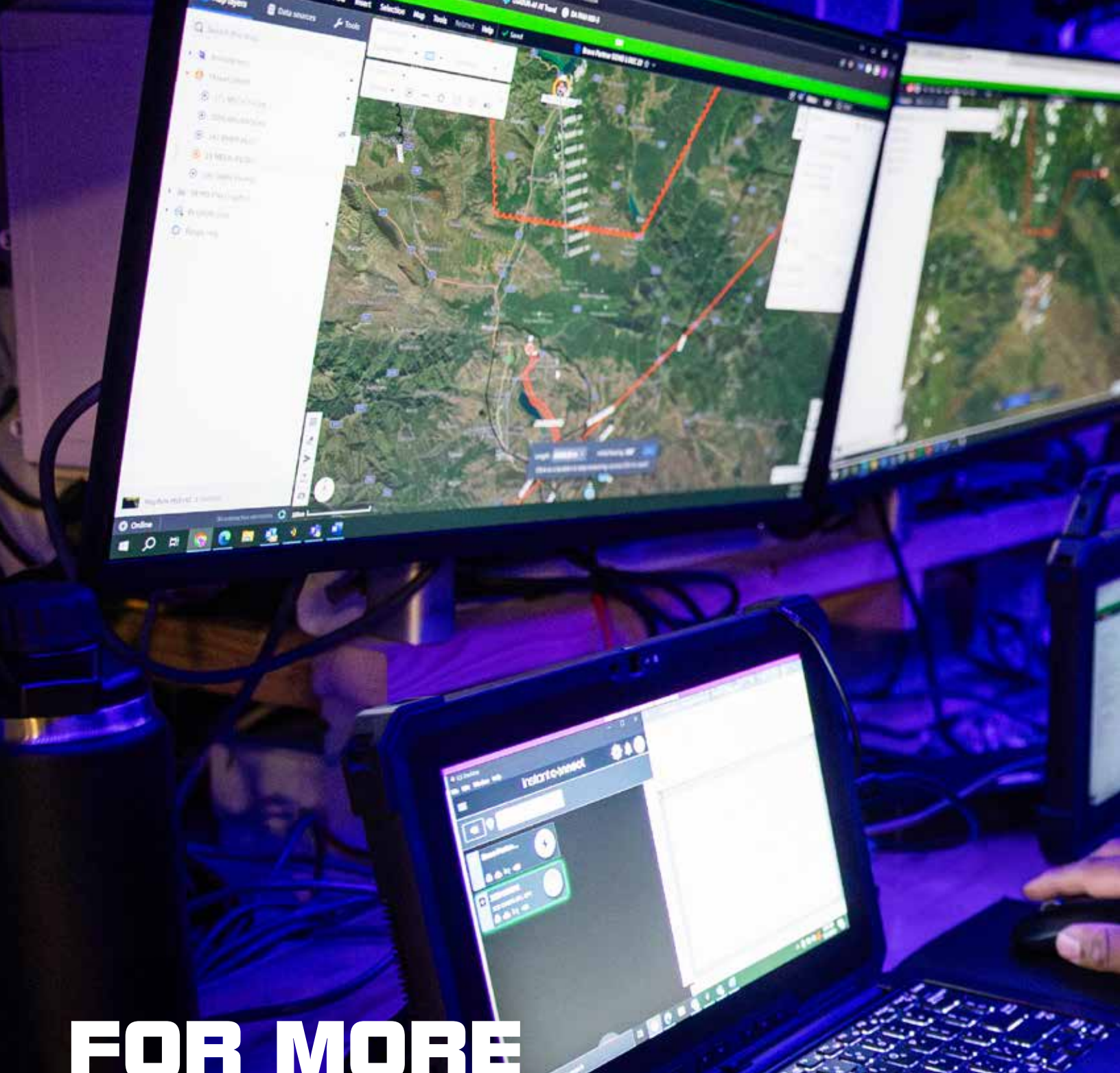
ARMY NETWORK MODERNIZATION STRATEGY LINE OF EFFORT

UNIFIED NETWORK	COMMON OPERATING ENVIRONMENT	JOINT & COALITION INTEROPERABILITY	CP MOBILITY/SURVIVABILITY

ACRONYMS

A
Advanced Field Artillery Tactical Data System (AFATDS)
Air to Ground Networking Information System (AGNIS)
Air and Missile Defense Workstation (AMDWS)
Army Key Management System (AKMS)
Army National Guard (ARNG)
Android Team Awareness Kit (ATAK)
At The Halt (ATH)
Automated Communications Engineering Software (ACES)

B
Battle Command Common Services (BCCS)
Communications, Command, and Control Leadership Board (C3LB)
Battlefield Video Teleconference (BVTC)
Beyond Line Of Sight (BLOS)
Brigade Combat Team (BCT)
Blue Force Tracker (BFT)

C
Campus Wide Local Area Network (CWLAN)
Capability Set (CS)
Coalition Joint Spectrum Management Planning Tool (CJSMPT)
Combat Camera (COMCAM)
Combat Net Radio (CNR)
Combat Survivor Evader Radio (CSEL)
Combined Enterprise Regional Information Exchange (CENTRIX)
Command and Control (C2)
Command and Staff Palletized Airborne Node (CASPAN)
Command, Control, Communications, Computers, Cyber, Intelligence,
   Surveillance, and Reconnaissance (C5ISR)
Command Post Local Area Network (CP LAN)
Command Post Computing Environment (CPCE)
Command Post Display System (CPDS)
Command Post Integrated Infrastructure (CPI2)
Command Post Support Vehicle (CPSV)
Commercial Coalition Equipment (CCE)
Commercial Internet and Phone (COM-IP)
Commercial-Off-The-Shelf (COTS)
Commercial Solutions for Classified (CSfC)
Common Access Card (CAC)
Common Hardware Systems (CHS)
Common Operating Environment (COE)
Common Operational Picture (COP)
Communications Security (COMSEC)
Continental United States (CONUS)

D
Defense Enterprise Computing Centers (DECC)
Defense Information Systems Network (DISN)
Defense Readiness Reporting System-Army (DRRS-A)
Defensive Cyber Operations (DCO)
Department of Defense (DoD)
Dependent Airborne Node (DAN)
Deployable Ku Band Earth Terminals (DKET)
Developmental Operations (DevOps)
Disaster Incident Response Emergency Communications Terminal (DIRECT)
Distributed Common Ground System-Army (DCGS-A)
Division Hub Node (DHN)

E
Electronic Causality Report (ECR)
Electronic Warfare (EW)

Electronic Warfare Planning and Management Tool (EWPMT)
Embedded Cryptographic Modernization Initiative (ECMI)
End of Life (EOL)
Enroute Mission Command (EMC)
Enterprise Over The Air Management (eOTAM)
Environmental control units (ECUs)
Expeditionary Signal Battalion (ESB)
Expeditionary Signal Battalion-Enhanced (ESB-E)
Extended Range Cannon Artillery (ERCA)
Extended Range Guided Multiple Launch Rocket System (ER-GMLRS)
Extreme Data Rate (XDR)
Extremely High Frequency (EHF)

F
Fire Support Command and Control (FSC2)
First Unit Equipped (FUE)
Fiscal Year (FY)
Fixed Installed Satellite Antenna (FISA)
Forward Entry Devices (FED)
Force XXI Battle Command Brigade and Below (FBCB2)
Forward Observer System (FOS)

G
General Fund Enterprise Business Systems (GFEBS)
Global Agile Integrated Transport (GAIT)
Global Broadcast Service (GBS)
Global Combat Support System-Army (GCSS-Army)
Global Information Grid (GIG)
Global Rapid Response Information Package (GRRIP)
Global Response Force (GRF)
Government-Off-The-Shelf (GOTS)
Gun Display Unit - Replacement (GDU-R)

H
Hand Held (HH)
Handheld, Manpack, and Small Form Fit (HMS)
Helicopter and Multi Mission Radios (HAMMR)
High-Altitude Electromagnetic Pulse (HEMP)
High Capacity Line Of Sight (HCLOS)
High Frequency (HF)
High Mobility Multipurpose Wheeled Vehicle (HMMWV)

I
Information Assurance (IA)
Integrated Personnel and Pay System-Army (IPPS-A)
Information Repository (IR)
Integrated Support System (ISS)
Integrated Tactical Network (ITN)
Integrated Visual Augmentation System (IVAS)
Integrated Tactical Networking Environment (ITNE)

J
Joint Automated Deep Operations Coordination System (JADOCS)
Joint Battle Command-Platform (JBC-P)
Joint Enterprise Network Manager (JENM)
Joint Forcible Entry (JFE)
Joint Incident Site Communication Capability (JISCC)
Joint Network Node (JNN)
Joint Tactical Networking Center (JTNC)
Joint Tactical Network Environment Network Operations Toolkit (J-TNT)

K
Key Management Infrastructure (KMI)

L
Lightweight Forward Entry Device (LFED)
Line Of Sight (LOS)
Local Area Networks (LANs)
Long-Range Precision Fires (LRPF)
Low Rate Initial Production (LRIP)

M
Management Client (MGC)
Manpack (MP)
Medical Communication for combat Casualty Care (MC4)
Military Information Support and Operation (MISO)
Mission Command (MC)
Mission Partner Environment (MPE)
Mobile User Objective System (MUOS)
Modular Communications Node - Advanced Enclave (MCN-AE)
Modular Radio Architecture (MRA)
Mounted Computing Environment (MCE)
Mounted Family of Computer Systems (MFoCS)

N
National Security Agency (NSA)
Network Cross-Functional Team (N-CFT)
Network Extension Packages (NEP)
Network Integration Technology Enhancement (NITE)
Network Operations (NetOps)
NetOps and Security Center (NOSC)
NOSC-Lite (NOSC-L)
Next Generation Load Device (NGLD)
Night Vision Device (NVD)

O
On-The-Move (OTM)

P
Point of Presence (PoP)
Positioning, navigation, and timing (PNT)
Precision-Fires Dismounted (PF-D)
Precision Strike Missile Program (PrSM)
Program Executive Office Command, Control and
    Communication-Tactical (PEO C3N)
Program Management Office Network Enablers (PMO Net E)
Project Manager Mission Command (PM MC)
Project Manager Tactical Radios (PM TR)
Project Manager Tactical Network (PM TN)
Projectile Tracking System (PTS)
Program of Record (PoR)

R
Regional Hub Nodes (RHN)
Remote Desktop Protocols (RDPs)
Rifleman Radio (RR)
Ruggedized Application Platform-Tactical Radio (RAP-TR)

S
Satellite Broadcast Manager (SBM)
Satellite Communications (SATCOM)
Satellite Transportable Terminal (STT)
Satellite Transportable Terminal Plus (STT+)
Secure High Assurance Inline Encryption Link Device (SHIELD)
Secure Internet Protocol Router (SIPR)
Secure Internet Protocol Router Network (SIPRNET)
Secure, Mobile, Anti-Jam, Reliable, Tactical - Terminal (SMART-T)
Signal Operating Instructions (SOI)
Single Channel Ground Airborne Radio System (SINCGARS)

Simple Key Loader (SKL)
SIPR/NIPR Access Points (SNAP)
Situational Awareness (SA)
Software Communications Architecture (SCA)
Software Development Kit (SDK)
Soldier Network Extension (SNE)
Soldier Radio Waveform (SRW)
Size, Weight and Power (SWaP)
Special Purpose Integrated Remote Intelligence Terminal (SPIRIT)
Special Operations Command (SOCOM)
Standard Tactical Entry Point (STEP)
Super High Frequency (SHF)
Sustainment Tactical Network (STN)
Systems Planning Engineering and Evaluation Device (SPEED)

T
Tactical Communications Marketplace (TCM)
Tactical Communication Node (TCN)
Tactical Command Post (TAC)
Tactical Communication Node-Lite (TCN-L)
Tactical Defensive (Cyber Operations) Infrastructure (TDI)
Tactical Digital Media (TDM)
Tactical Hub Node (THN)
Tactical Internet (TI)
Tactical Mission Command (TMC)
Tactical Network Initialization & Configuration (TNIC)
Tactical Operation Center (TOC)
Tactical Radio Report (TRR)
Tactical Server Infrastructure (TSI)
Transportable Tactical Command Communications (T2C2)
Tactical Theater Signal Brigade (TTSB)
Tri-band Line of Sight (TRILOS)
Tobyhanna Army Depot (TYAD)
Troposcatter Transmission (TROPO)

U
Ultra High Frequency (UHF)
Unified Network Operations (UNO)
Unified Trouble Ticketing System (UTTS)
Unit Reference File (URN)
Unit Task Organization (UTO)
Unit Task Reorganization (UTR)
United States Message Text Format (USMTF)
Unmanned Aircraft System (UAS)

V
Variable Message Format (VMF)
Vehicle Integration for C4ISR/EW Interoperability (VICTORY)
Vehicle Wireless Package (VWP)
Very Small Aperture Terminal (VSAT)
Voice over Internet Protocol (VoIP)

W
Wideband Global SATCOM (WGS)
Wideband Networking Waveform (WNW)
Warfighter Information Network-Tactical (WIN-T)
Warfighter Initialization Tool (WIT)

FOR MORE
INFORMATION

PEO C3N
PROGRAM EXECUTIVE OFFICE COMMAND, CONTROL, COMMUNICATIONS, AND NETWORK

U.S. ARMY

Approved for public release; distribution is unlimited. December 2024