TABLE OF CONTENTS

A | JTNC
- Joint Tactical Networking Center (JTNC) 6-7

B | PM MC
- Command Post Computing Environment (CP CE) 8-9
- Fire Support Command and Control (FSC2) 10-11
- Joint Battle Command-Platform (JBC-P) 12-13
- Mounted Computing Environment (MCE) 14-15
- Strategic Mission Command (SMC) 16-17
- Mission Command Cyber (MC Cyber) 18-19
- Command Post Integrated Infrastructure (CPI2) 20-21

C | PMO NET E
- Common Hardware Systems (CHS) 22-23
- Communications Security (COMSEC) 24-25
- MilTech Solutions 26-27

D | PM TR
- Integrated Tactical Network (ITN) 28-29
- Handheld, Manpack, and Small Form Fit (HMS) 30-31
- Helicopter and Multi Mission Radios (HAMMR) 32-33
- Waveforms 34-35

E | PM TN
- Mission Network 36-37
- Tactical Network Transport at-the-halt 38-39
- Tactical Network Transport on-the-move 38-39
- Regional Hub Node (RHN) & Global Agile Integrated Transport (GAIT) 40-41
- SigMod 42-43
- Enroute Mission Command (EMC) 44-45
- Terrestrial Transmission Line Of Sight (TRILOS) 46-47
- Troposcatter Transmission (Tropo) 48-49
- Secure WI-FI 50-51
- Commercial Coalition Equipment (CCE) 52-53
- Modular Communications Node-Advanced Enclave (MCN-AE) 54-55
- Disaster Incident Response Emergency Communications Terminal (DIRECT) 56-57
- Area Common User System Modernization (ACUS MOD) 58-59

Satellite Communications
- Transportable Tactical Command Communications (T2C2) 60-61
- Scout 62-63
- Global Rapid Response Information Package (GRRIP) 64-65
- Secure, Mobile, Anti-Jam, Reliable, Tactical-Terminal (SMART-T) 66-67
- Phoenix 68-69
- Global Broadcast Service (GBS) 70-71
- Deployable Ku Band Earth Terminals (DKET) 72-73
- SIPR/NIPR Access Points (SNAP) 74-75
- Tactical Cyber and NetOps 76-77
- Unified Network Operations (UNO) 78-79
- Joint Enterprise Network Manager (JENM) / Joint Tactical Network Environment Network Operations Toolkit (J-TNT) 78-79

ACRONYMS
Headquartered at Aberdeen Proving Ground, Maryland, Program Executive Office Command, Control, Communications-Tactical (PEO C3T) develops, acquires, fields and supports the Army’s tactical network, a critical modernization priority. PEO C3T delivers the hardware and software required to provide Army formations with an expeditionary, mobile, simple to use and hardened tactical network.

The reach of government and contractors of PEO C3T throughout the United States.
PEO C3T is supporting the Army’s new network modernization strategy with a commitment to deliver a tactical network that ensures the Army, with Unified Action partners, can prepare for war and fight and win against any adversary in the most challenging contested and congested electromagnetic spectrum and cyber environments. The end-to-end tactical modernization approach is designed to integrate unified network transport, shared data and services including the servers and hardware, and a set of applications and network management tools built upon a common, open, and modular software framework.

PEO C3T manages more than 53 key acquisition programs executing more than $2 billion annually with a workforce of more than 1600 employees. The organization provides operational units with radios, computers, servers, apps, and other hardware and software required for their missions, while also integrating those systems to function as cohesive capability sets. In FY18 the PEO modernized 285 Army, Army Reserve and Army National Guard units with updated network technology. Units included Brigade Combat Teams, Security Force Assistance Brigades (SFABs) and signal, logistics, aviation and support elements. Centered upon the proven industry practice of developmental operations (DevOps), the modernization strategy is placing developers side-by-side with Soldiers and commanders in operational units. DevOps enables the Army to evaluate potential technology concepts and solutions earlier and more frequently, incorporating real-time operational feedback and generating requirements that enable and empower innovation. Over the past year, PEO C3T has used the DevOps construct to better assess the baseline tactical network, introduce new network enhancement alternatives and gather Soldier-informed feedback and technical data.

PEO C3T is working closely with the Network Cross Functional Team (N-CFT) to modernize the network across four lines of effort: Unified Network Transport; Common Operating Environment; Joint Force and Coalition Interoperability; and Command Post Mobility and Survivability. Key Army network modernization efforts include fielding standard mission command hardware and software across all component formations, accelerated fielding of the Joint Battle Command Platform mounted situational awareness and communications system, fielding advanced tactical data radios and modernizing the satellite communications systems.

PEO C3T, with the N-CFT, is incorporating new commercial off-the-shelf (COTS) components and transport capabilities to enable network communications in disconnected, intermittent and limited bandwidth (DIL) network transport environments. This effort, termed the Integrated Tactical Network (ITN), provides a simplified, independent, mobile network solution that is available down to the small-unit dismounted leader to facilitate mission command, situational awareness and air-to-ground integration. ITN will provide commanders with resilient communications that are part of their Primary, Alternate, Contingency and Emergency (PACE) communications plan.

Commercial cellular networks are other options under consideration as part of a PACE plan. Commercial standards such as 4G/LTE and Wi-Fi, while not currently hardened against the kind of full spectrum Electronic Warfare (EW) environment envisioned, are being adapted to supplement and thicken the network and decrease the time it takes to get command posts up and running. Emerging commercial satellite communications (SATCOM) constellations promising high bandwidth anywhere across the globe are another key element of the modernization vision.

In addition to EW threats, defense against cyber-attack and intrusion remains a critical underpinning of the strategy. Recently the Army established new program efforts including cyber situational understanding (Cyber SU) to aid operational units’ understanding of the tactical network threat environment.

Moving forward, experiments and evaluations will focus on driving network design changes across Security Force Assistance Brigades (SFABs), Infantry, Stryker and Armor Brigade Combat Teams, and tailoring the network and command post configurations to the unique needs of each formation. The output of these efforts will continue to generate informed network capability requirements, while enabling the Army and its industry partners to evolve the network at the pace of warfighter demands and commercial innovation and to meet emerging threats.
To ensure interoperable, secure, and affordable waveform and wireless communications by recommending standards, conducting compliance and certification analyses in accordance with DoD policies, and maintaining a DoD Waveform Information Repository (IR).
**DESCRIPTION**

The JTNC, chartered by the Under Secretary of Defense Acquisition, Technology & Logistics (USD (AT&L)) certifies secure, reusable software waveforms based on government-controlled open architecture that encourages a highly competitive, cost effective and interoperable networking environment. JTNC enables service cost savings through waveform reuse by reducing software procurement schedules and development time, and ultimately speeding capabilities to warfighters. It improves Joint Command and Control (C2) capabilities by promoting effective information sharing and integration of C2 capabilities through the more efficient use of resources, common architectures, standards, software reuse and data exposure. JTNC provides government and industry access to reusable software in support of development activities.

**CAPABILITIES**

To address the changing Army tactical communications modernization needs, the JTNC is developing a tactical communications vendor product capability characterization process for vendor Commercial off-the-shelf (COTS)/Non-developmental Item (NDI) tactical communication products. The process will provide an earlier assessment of which COTS/NDI products would benefit the warfighter needs. The JTNC is also developing a tactical communications marketplace, which is an on-line resource for commercial vendors designed to showcase their tactical communications product offerings. The marketplace will enable government buyers (acquisition authorities) to scroll through the selection of available products (based on desired search criteria) and browse product reviews based on JTNC analysis. This initiative will promote the receipt and analysis of COTS/NDI waveforms, which will speedup innovative industry ideas and delivery to the services.

The JTNC also operates and maintains the DoD Waveform Information Repository (IR), a cyber-hardened repository for software code and relevant technical documentation for reuse by government and software developers. The DoD Waveform IR maintains an online interface accessible for registered users (www.dodir.mil), which features the product catalog, service and support, user registration, and contact information. JTNC performs technical analyses of candidate waveform and wireless communications products to preliminary determine if they meet DoD standards and policies for interoperable and secure joint tactical networking. The waveforms analysis aligns with DoD Instruction 4630.09, Communication Waveform Management and Standardization, dated 15 July 2015, and is intended to provide DoD program managers and DoD leaders with the information necessary for deployment and reuse on new radio platforms.

The JTNC provides a validated open architecture framework (e.g. Software Communications Architecture (SCA)) that identifies standard non-proprietary interfaces that separate the waveform/network manager software from the radio set, permitting common waveforms and network managers to be deployed across multiple radio sets. Additionally, the JTNC supports the various DoD agencies overseeing the protection of wireless communications critical technologies exported under commercial and/or Foreign Military Sales and licenses.

As radio technology quickly advances, the JTNC continues to focus attention to the critical aspects of command and control communication devices, more specifically the waveform of tomorrow.
The Command Post Computing Environment (CPCE), under the direction of Product Manager Tactical Mission Command (TMC), provides a software infrastructure framework (common interface, data and services) upon which current Warfighter capabilities can be converged and future capabilities can be built. CP CE is the primary computing environment under the Common Operating Environment (COE) initiative, a major Army network modernization strategy line of effort of the Network Cross-Functional Team (N-CFT). CP CE is the central computing environment developed to support command posts and combat operations, and it will be interoperable with mounted and mobile/Handheld systems.

- Systematic
- Futures Skies
- Bowhead
- CACI
- AASKI
- General Dynamics Mission Systems

CONGRESSIONAL LOCATIONS

KEY CONTRACTORS

PAGE 8 // PROGRAM EXECUTIVE OFFICE COMMAND CONTROL COMMUNICATIONS-TACTICAL
DESCRIPTION
CP CE will eliminate stove-piped legacy systems and provide an integrated, interoperable, cyber-secure and cost-effective computing infrastructure framework for multiple warfighting functions. CP CE will provide programs of record (PoRs) with a core infrastructure, including a common operating picture (COP) tool, common data strategy, common applications such as mapping and chat, common hardware configurations and common look and feel (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. CP CE’s acquisition goals include acquisition agility, open system architectures (OSAs), reduced lifecycle costs and a cyber-hardened foundation for applications and services.

CAPABILITIES
• CP CE provides an integrated mission command capability across command post and platforms, through all echelons, and provides simplicity, intuitiveness, core services and applications, and warfighter functionality in the areas of fires, logistics, intelligence, airspace management and maneuver.

• CP CE offers a common geospatial solution (map) and common data services, including an extensible database and data persistence. The system is designed to reduce the training burden on Soldiers. The Integrated Software Development Kit (ISDK) allows external Programs of Record (PoRs) the ability to integrate new capabilities without rebuilding common components.

• CP CE software will reside on a converged commercial off-the-shelf (COTS) hardware solution called the Tactical Server Infrastructure (TSI) stack, which hosts multiple software infrastructure components including Active Directory, Microsoft Exchange, SharePoint, Defensive Cyber Operations (DCO) tools, SQL databases and a Voice over Internet Protocol (VoIP) tool. This enterprise software is tightly coupled with, and engineered for, specific TSI hardware using virtual machine (VM) technology. It must serve as the basis for all other warfighting functions and mission command system software loaded on the server.
Fire Support Command and Control (FSC2) empowers commanders to plan and execute the delivery of lethal fires and effects by providing capabilities to employ joint digital fires, enhance situational awareness and increase collaboration.
DESCRIPTION
FSC2 provides Army, joint and coalition commanders with the capability to plan, execute and deliver both lethal and non-lethal fires and effects. 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)** provides fully automated support for planning, coordinating, controlling and executing fires and effects, including mortars, field artillery cannons, rockets and missiles, close air support, attack aviation and Naval surface fire-support systems. AFATDS is the primary command and control system for Long-Range Precision Fires (LRPF) Cross-Functional Team (CFT) initiatives, such as Extended Range Cannon Artillery (ERCA), Extended Range Guided Multiple Launch Rocket System (ER-GMLRS), Precision Strike Missile Program (PrSM) and Projectile Tracking System (PTS).
- **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.
- **Lightweight Forward Entry Device (LFED)** hosts the Forward Observer System (FOS) software, which enables 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. It will be replaced by Precision Fires-Mounted (PF-M) beginning in FY21.
- **CENTAUR** is the lightweight technical fire direction system that provides an automated cannon ballistic firing solution to the Fire Direction Centers (FDCs). Its primary function is a secondary technical calculation check for AFATDS or manual calculations.
- The **Profiler** weather system improves artillery accuracy by providing meteorological (MET) data, which is one of five requirements for accurate predicted fires. Profiler provides MET information to field artillery assets via AFATDS. Weather information is received via the Weather Data download site or the Global Broadcast Satellite (GBS), and computations provide correction information along the projectile trajectory and within the target area.
- **Joint Automated Deep Operations Coordination System (JADOCS)** is 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. JADOCS provides timely, accurate, detailed battlespace view for target nomination and vetting, target execution and coordination, air operations information, intelligence operations information, battle damage assessment and campaign plan.
Joint Battle Command-Platform (JBC-P) is the Army’s next-generation friendly force tracking system, equipping Soldiers with a faster satellite network, secure data encryption and advanced logistics.

- COMTECH
- ACE Electronics Defense
- DRS Technology
- General Dynamics
- ViaSat
- Telesis
- INMARSAT Gov.
DESCRIPTION
JBC-P is the Army’s next-generation friendly force tracking system, equipping Soldiers with a faster satellite network, secure data encryption and advanced logistics. Fielded to the first unit equipped in May 2015, JBC-P includes an intuitive interface with features like touch-to-zoom maps and drag-and-drop icons. JBC-P will be interoperable with the Nett Warrior handheld device, managed by PEO Soldier, delivering situational awareness capabilities to dismounted Soldiers. JBC-P incorporates the common hardware solution known as the Mounted Family of Computer Systems (MFoCS), which encompasses standardized tactical computers that are scalable and tailorable to the mission and vehicle. Ranging in options from a detachable tablet to a fully loaded, vehicle-mounted workstation, MFoCS can also run other software applications, reducing size, weight and power (SWaP) demands. JBC-P builds on the situational awareness capability known as Force XXI Battle Command Brigade and Below/Blue Force Tracking (FBCB2/BFT), which is integrated on more than 120,000 platforms and is fielded or authorized to every brigade combat team in the Army.

CAPABILITIES
- Increased accuracy and density of situational awareness to further mitigate risk of fratricide
- Orders, graphical overlays, friendly, hostile, neutral, unknown, and non-combatant situational awareness
- Free draw, free text, chat and combat messages
- Sensor integration to enable capability to pinpoint location
- Hybrid network
- Improved user interface
- Electronic Causality Report (ECR)
- Improved route planning

A | Mounted Family of Computer Systems (MFoCS) will serve as the hardware provider for the MCE, Android-based software.
B | Soldier working on JBC-P at Network Integration Evaluation 18.2 at Doña Ana Range, N.M., Oct. 30. Photo by: Miguel De Santiago / Special to the Fort Bliss Bugle.
C | Soldier assigned to the 2nd Battalion, 5th Cavalry Regiment, 1st Armored Brigade Combat Team, 1st Cavalry Division tracks three different companies’ movement using the blue force tracker during the battalion’s command post exercise in Mihail Kogalniceanu, Romania, August 16, 2018.
The Mounted Computing Environment (MCE) will provide a common set of applications and services as part of the Army’s Common Operating Environment (COE) to enable mission command on ground platforms. MCE will enable modular and scalable solutions allowing for the convergence of current software systems and the agile development and certification of new on-the-move capabilities.
DESCRIPTION
As one of six computing environments that make up the Army-wide Common Operating Environment (COE), MCE embraces a commercially based set of standards, a common understanding of data, and a common map to enable integrated applications for development by government and industry partners. MCE will provide data services that work on the Army’s tactical radio networks and network-aware services that enable mission command data to flow throughout the disadvantaged, intermittent and latent network environments among dismounted Soldiers, vehicles and command posts.
MCE uses the same infrastructure as the Command Post Computing Environment (CP CE) and integrates it onto the Mounted Family of Computer Systems (MFoCS), along with the Android operating system framework for applications hosting and simplified user experience. This approach enables tech-savvy Soldiers to rapidly learn and become proficient on MCE applications with minimal training. It will also improve interoperability with command posts and reduce duplication and complexity of software development and configuration management for both MCE and CP CE applications. MCE applications will work seamlessly with the CP CE applications, similar to how commercial programs are integrated across standard computers, tablets and smartphones. MCE will be fully compatible with existing platform-based systems while improving upon the cyber posture and being extensible to meet evolving enemy threats. MCE infrastructure will provide a framework that will allow seamless integration of other third-party applications.

CAPABILITIES
• Provides operating systems, common applications, software development kits (SDKs) and standards to implement mission command
• Establishes secure applications that are interoperable with existing mission command systems and allow seamless information exchange across all echelons for a complete situational awareness (SA) picture down to the tactical edge
• Provides an SDK framework that allows for seamless integration of third-party applications built by other programs of record (PoRs) and contractors
• Enables mission command on-the-move by providing an environment for an integrated suite of platform-based mission command applications and services
• Eliminates redundant hardware, streamlines product development and consolidates capabilities
• Optimized for use on the existing MFoCS and Blue Force Tracking (BFT) 2 network
• Provides standard interfaces to meet the Vehicle Integration for C4ISR/EW Interoperability (VICTORY) technical specifications
Strategic Mission Command (SMC) develops, integrates, fields and supports the Army’s core mission command collaborative environment and maneuver applications to enable operating force commanders to make timely and effective decisions within the Army, joint and coalition environments. Product Director SMC will reach full deployment and transition all products to sustainment in FY19.

- General Dynamics
- CACI
- ESP
- Future Skies
- Bowhead
DESCRIPTION
SMC provides interoperable hardware and software solutions to the Army, joint and coalition partner communities.

CAPABILITIES
- **Global Command and Control System-Army** (GCCS-A) is the Army’s strategic and theater command and control (C2) system. It fulfills the need for critical automated C2 to enhance Soldiers’ capabilities throughout the spectrum of conflict during joint and combined operations.
- **Common Software** (CS) is a suite of 13 individual products that, when combined, provide the binding agent for interoperability among the Army’s C4ISR systems.
- **The Command Post of the Future** (CPOF) is a decision support system, providing situational awareness (SA) and collaborative tools for tactical decision making, planning, rehearsal, and execution management from corps to company level.
- **WAVE** is a commercial-off-the-shelf (COTS) Voice over Internet Protocol (VoIP) tool that provides interoperable voice support to CPOF.
- **Command Web** (CW) is an extensible web framework environment that houses C2 lightweight web applications called “widgets” to facilitate the fusion of operations information and engineer capabilities to provide a more complete SA picture and engineer staff capabilities.
- **Battle Command Common Services** (BCCS) and **Tactical Server Infrastructure** (TSI) provide a powerful and capable server suite for virtualizing mission command focused applications while ensuring commonality to the command post hardware infrastructure.
Mission Command Cyber (MC Cyber) designs, develops and deploys cyber capabilities to the Army to establish cyber operational overmatch. MC Cyber delivers capabilities to corps and brigades at the tactical edge that allow warfighters to understand and depict cyberspace while defending friendly key cyber terrain.

- CACI
- Polaris Alpha
- Adorama
- General Dynamics
- Dell
DESCRIPTION

MC Cyber’s agile acquisition and integration processes achieve both near- and long-term capability development to ensure dominance in the cyber battlefield.

CAPABILITIES

- Tactical Defensive (Cyber Operations) 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 addresses this need by pre-positioning DCO tools onto dedicated computer and storage resources residing at echelons corps and below. The TDI system is physically and logistically converged with the Tactical Server Infrastructure (TSI) to minimize size, weight, and power (SWaP) requirements in a tactical operations center (TOC) or tactical command post (TAC).

- Cyber Situational Understanding: Cyber SU will ingest, normalize, correlate, and analyze disparate data from multiple Army programs of record (PORs) within an Army TAC, including Command Post Computing Environment (CP CE), Distributed Common Ground System-Army (DCGS-A), Electronic Warfare Planning and Management Tool (EWPMT), TDI, and Tactical Network (TN).

- Tactical Digital Media: Public Affairs (PA) teams are often dispatched with combat patrols and small units that deploy to remote locations. Tactical Digital Media (TDM) kits allow these teams to gather, process and deliver audio files, digital imagery and visual media in austere environments with cameras and video equipment, laptops, night-vision devices and audio gear. TDM aids globally deployed Combat Camera (COMCAM) teams, PA detachments and Military Information Support and Operation (MISO) teams operating from TCPs, forward operating bases (FOBs), combat outposts and forward deployed combat patrols.
Command Post Integrated Infrastructure (CPI2), aligns to the Army’s Command Post Mobility/Survivability level of effort, addresses capability shortfalls outlined in the Army’s Command Post (CP) Directed Requirement by collaborating with government and industry partners to design, prototype, and integrate mobile, survivable and agile CP solutions.
DESCRIPTION
The CPI2 program has the mission to develop modern and mobile command posts (CPs), which are the field headquarters where Soldiers, the network, procedures and processes, and information systems come together. The mobile CPs replace large legacy CPs that are vulnerable because of their physical signature, limited mobility and lack of standardization. The program provides integrated infrastructure via a mix of vehicle platforms and shelter systems that enable CP functionality, increasing survivability through mobility and rapid displacement of the CP infrastructure.

CAPABILITIES
CPI2 leverages improvements in technology to reduce the current CP footprint and improve agility. It consists of the integration of approved and fielded mission command information systems, government-off-the-shelf (GOTS) and commercial off-the-shelf (COTS) technology that support the operational needs of the corps, division and brigade combat team (BCT) main and tactical CPs, and the BCT battalion CPs. The centerpieces of CPI2 are the Mission Command Platform (MCP) and Command Post Support Vehicle (CPSV). CPI2 also provides all the ancillary equipment for fully outfitting the mobile CP, including the CPI2 Integrated Support System (ISS), tents, environmental control units (ECUs), power generation, displays, tables and chairs.

• Mission Command Platform (MCP) The MCP provides digitally connected workstations to support staffs at CPs, as well as command groups at corps, division, and BCT. The MCP uses current program of record (PoR), GOTS and COTS systems to plan, prepare, execute and assess operations.

• Command Post Support Vehicle (CPSV) The CPSV hosts mission command servers, radios, local area network (LAN) systems and a Unified Voice Management System (UVMS) for conferencing, access to tactical voice radio, Voice over Internet Protocol (VOIP) telephone, and radio cross banding.

• Integrated Support System (ISS) CPI2 will develop or acquire the Command Post Display System (CPDS) and UVMS. The CPDS, with its accompanying software, will support enhanced collaboration and communication by allowing the commander and staff the option to view multiple common operating pictures (COPs) simultaneously. The UVMS provides data communication exchange between Army standard network and radio protocols within, and between, the mobile CPs.

A | The 1st Stryker Brigade Combat Team, 4th Infantry Division conduct operations at National Training Center, Fort Irwin, California. This represents the desired mobility from the CPI2 program.

B | The 4th Infantry Division demonstrates a Command Post Platform-Improved at Fort Carson, Colorado. It represents a potential CPI2 CPSV solution.

C | Soldiers with the 1st Armored Division, 2nd Armored Brigade Combat Team’s 1st Squadron, 1st Cavalry Regiment Main plan their mission from inside the Lightweight Mobile Command Post TAC during the Network Integration Evaluation/Army Warfighter Assessments.
Common Hardware Systems (CHS) acquires and supports sustainment of highly flexible, cost effective, common, and simplified non-developmental, commercial information technology solutions that improve interoperability and connectivity on the battlefield while garnering efficient competition to enable the latest commercial technology solutions to meet tactical/operational requirements.
DESCRIPTION
CHS coordinates across tactical programs providing consolidated procurement and sustainment support of modified commercial off the shelf information technology. The program portfolio ensures configuration and obsolescence management by continually updating new contract items ensuring modern, emerging technologies resulting in overmatch capabilities for warfighters. New this fiscal year is the fifth generation contract, referred to as CHS-5. The CHS-5 contract allows Army Weapon System Programs to rapidly buy commercial information technology (IT) equipment like laptops, servers, routers, switches and integrated solutions in large quantities and at discounted prices. CHS provides state-of-the-art computing and networking equipment that improves connectivity, interoperability, logistics and maintenance support to Soldiers, and the program is positioned as the Army’s primary organization to oversee commercial information technology (IT) hardware for the Army’s tactical network.

The contract is a Single Award, Indefinite Delivery Indefinite Quantity contract having a five-year Period of Performance, with a $3.9 billion ceiling, for the rapid procurement of total life cycle system management solutions in support of tactical programs. 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. The CHS-5 contract requires the prime contractor to establish a Public Private Partnership with Tobyhanna Army Depot (TYAD), facilitating product support for programs procuring hardware via CHS-5 and having core logistics capability requirements. This partnership leverages TYAD and CHS innovation and resources providing the best value to the warfighter. The CHS-5 contract also provides the Government with an increased ability to perform supply chain risk management, critical functionality analysis of critical components, critical program information assessment and implementation of other protection measures contained in Program Protection Plans. This contract feature strengthens the Army’s cybersecurity posture while protecting the tactical network.

Other enhancements for CHS-5 include a pre-negotiated pricing schedule for the life of the contract; 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 Data Packages based on competitive pricing.
Communications Security (COMSEC) develops, tests, procures, fields and sustains COMSEC solutions to secure the Army’s network (tactical through enterprise).
DESCRIPTION

Under the umbrella of the National Security Agency (NSA), the Army provides all users from Enterprise down to tactical units with secure organic key management (ordering, generation, distribution, destruction).

The Army Key Management Infrastructure (AKMI) consists of three subcomponents: Management Client (MGC), Automated Communications Engineering Software (ACES) and Next Generation Load Device (NGLD). AKMI provides a system for distribution of COMSEC, electronic protection, mission initialization data, and Signal Operating Instructions (SOI) information from the planning level to the point of use in support of current, interim, and objective force structure. AKMI introduces capabilities and processes to transform operations from manual to secure automated distribution of keys and firmware directly to end devices.

New and emerging architectures, cease key dates, and DoD/Army policy are driving the need to replace legacy devices with technically advanced (network-centric GIG compliant) modern devices that incorporate Chairman of the Joint Chiefs and Joints Requirements Oversight Council directed cryptographic standardization, Key Management Infrastructure (KMI) and network centric performance capabilities. This enables the Army to equip the force with critical cryptographic solutions and services during peacetime, wartime, and contingency operations.

CAPABILITIES

• **Cryptographic Mission Planner:** Provides Crypto network planning; generates SOI data; creates COMSEC key tags; supports emerging requirements.

• **Tier 3 Load devices:** Small, ruggedized design that allows loading of Cryptographic keys and mission data into SHIELD devices, radios, End Cryptographic Units, interfaces between key generation MGC, and Mission Planners.

• **Secure High Assurance In-line Encryption Link Device (SHIELD):** SHIELD encryption systems secure the Army’s data and voice communication networks. SHIELD encryption devices include in-line network and in-line media, link and trunk, secure voice, and Commercial Solutions for Classified.

• **Embedded Cryptographic Modernization Initiative (ECMI):** Retrofit of existing systems with embedded cryptographic capability to ensure they will be able to accept and utilize modern keying material.
Military Technical (MilTech) Solutions provides innovative collaboration and information sharing IT services and products that increase the efficiency and operational performance of the diverse DoD workforce.
DESCRIPTION
Military Technical (MilTech) Solutions is a fully reimbursable Non-Acquisition Category (ACAT) that provides collaboration technologies to connect the DoD community and close the gap between enterprise and tactical IT. MilTech uses a customer-funded approach that allows partnered organizations to pool resources and co-invest in technologies, reducing each partner’s individual costs while addressing critical organizational IT challenges.

CAPABILITIES
• milSuite: milSuite is a collection of secure, web-accessible online tools based on popular and highly used collaborative sites from the commercial web to provide social networking and collaboration behind the DoD firewall. The milSuite applications - milBook, milWiki, and milTube allow communities to build, share and connect across the DoD community.

• Knowledge Management: is a collection of GOTS and COTS tools that enable collaboration, information sharing and business process automation resulting in informed decision making. Foremost among these is Microsoft SharePoint, a collaboration platform; Green Force Tracker, a chat/instant messaging and presence/awareness capability; and Manpower Information Retrieval and Reporting System (MIRARS) for managing personnel accountability in emergency situations.

• Single Interface to the Field Information Technology Service Management (SIF ITSM): provides a multi-tenant ITSM tool on NIPR and SIPR used for C4ISR field support, failure reporting, asset management, help desk, service management, catalog and order tracking. SIF ITSM utilizes multiple interfaces including SharePoint, Quick Submit Forms, and the new Remedy SMART IT interface as well as providing robust reporting capabilities.

• Business Intelligence and Decision Support: provides capabilities aimed at transforming data into actionable information and facilitating data-driven decision making via big data/data warehousing. This identifies trends, costs, outcomes and risks via ad-hoc end-user reporting capabilities and data visualization.

• While MilTech primarily adapts COTS products to solve business challenges via a Software as a Service Model, MilTech also offers custom development and configuration services to include: website, portal, program and project management and knowledge management systems development.

A | MilSuite has more than 1,300,000 registered users from across the DoD with 15,000 users onboarding each month.
B | Over 30,000 SharePoint 2013 users from across the Army Acquisition Community.
C | Surpassed 67 million chat session on Green Force Tracker.
D | MilTech supports the Common Hardware Systems (CHS) Rapid Acquisition and Procurement Integrated Database System (RAPIDS), which provides an Amazon-like ordering platform leveraging SIF ITSM to procure assets from the CHS hardware item catalog while also supporting CHS order fulfillment processes.
The Integrated Tactical Network (ITN) provides a simplified, independent, mobile network solution that is available down to the small-unit dismounted leader to facilitate mission command, situational awareness, and air-to-ground integration. The ITN will provide commanders with resilient communications as part of their primary, alternate, contingency and emergency communications plan.
DESCRIPTION
The ITN is not a new or separate network but rather a concept that incorporates the Army’s current tactical network environment (applications, devices, gateways, and network transport) with commercial off-the-shelf components and transport capabilities to enable communications in disconnected, intermittent, and limited bandwidth environments. ITN is comprised of an integrated set of Leader Radios with advanced networking waveforms, gateways, Link-16 radios, small aperture satellite terminals, servers, applications and associated ancillary devices. These commercial components and current network systems offer commanders multipath communications diversity and will interoperate with current network systems. ITN aligns with the Army’s Unified Network Transport Level of Effort.

CAPABILITIES
• Operates in both a Secret and a Secure but Unclassified Network environment to allow data to be categorized in accordance with its classification and to enable greater information sharing with partner nations
• Simplifies training, set-up, and employment of the network
• Enables use of alternate transport including 4G/LTE
• Interoperates with current network systems to enable mission command systems used in command posts and on platforms.
• SBU operating environment long a concern as the secret classification of battlefield data has hindered coalition operations.

A | U.S. Army 1st Lt Michael Austin, a platoon leader for Attack Co., 1st Battalion, 503rd Infantry Regiment, uses an end user device to report information to his company commander through the Integrated Tactical Network during a live-fire exercise in Grafenwoehr, Germany, May 2, 2018.
B | Soldier uses an ITN system during air assault training as part of Exercise Saber Junction 2018 at the Grafenwoehr Training Area, Germany, Sept. 12, 2018.
C | Paratroopers with C Company, 1-508th Parachute Infantry Regiment (PIR), 82nd Airborne Division (Air Assault) assess the Integrated Tactical Network (ITN) while performing an air assault exercise in January 24, 2019 at Camp Atterbury, Indiana.
Handheld, Manpack and Small Form Fit (HMS) develops and produces affordable networking tactical radio systems that meet the requirements of the Army, Marine Corps, Navy, Air Force and Special Operations Command (SOCOM) and are interoperable with specified radios in the current forces.
DESCRIPTION
Handheld, Manpack and Small Form Fit (HMS) is a family of networking tactical radio systems that are interoperable with specified radios in the current forces. HMS provides joint interoperable connectivity to the tactical edge Soldier 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. The radios are scalable and modular Software Communications Architecture (SCA) compliant, enable net-centric operations, operate multi-band and multimode; and deliver reliable, secure tactical communications.

Full Rate Production (FRP)
Manpack Radios
- Manpack AN/PRC158, 2 Channel, Type 1 and Type 2, SRW, MUOS, SINCGARS, SATCOM (Harris)
- Manpack AN/PRC162, 2 Channel, Type 1 and Type 2, SRW, MUOS, SINCGARS, SATCOM (Rockwell Collins)

Low Rate Initial Production (LRIP) Leader Radio:
- AN/PRC-148C(v)6 (Thales), 2 Channel, SRW, SINCGARS, TSM (TM)
- AN/PRC-163(v)2 (Harris), 2 Channel, SRW, SINCGARS, TSM (TM)
- AN/PRC-154, 1 Channel SRW only
- AN/PRC-154A, 1 Channel SRW only

LRIP Manpack Radios:
- AN/PRC-155, 2 Channel, Type 1 and Type 2 (General Dynamics)

CAPABILITIES
- Simultaneous voice, data and video communications
- Increased throughput using networking waveforms

Mobile User Objective Systems (MUOS) for BLOS
- Manpack Routing and Retransmission (Crossbanding)
- Manpack Multi-Channel and Multi-Channel and Multi-Waveform operations
- Non Development Item increased functionality to include Size, Weight, and Power (SWaP) improvements, addition of a display for the Rifleman Radio, and additional waveforms (e.g. TACSAT IW for the Manpack)

PROJECT MANAGER
TACTICAL RADIOS
HANDHELD, MANPACK, SMALL FORM FIT (HMS)

A | Paratrooper with the 82nd Airborne Division’s 1st Brigade Combat Team leads fellow paratroopers back from a combined operation use Rifleman Radio for communications.
B | AN/PRC-163 (Harris); AN/PRC-148B/C (Thales).
C | AN/PRC-155 (v)2 (GD); AN/PRC-162 (v)1 (Rockwell Collins Inc.); AN/PRC-158 (v)3 (Harris)
D | 1st SFAB advisers conduct radio training before traveling to Kabul to advise Afghani National Army Security Forces on April 13, 2018.
Helicopter and Multi Mission Radios (HAMMR) encompasses the overarching Integrated Tactical Network (ITN), Security Forces Assistance Brigades. Air to Ground Networking Information System (AGNIS), Combat Survivor Evader Radio (CSEL), High Frequency Radios (HF), Integrated Visual Augmentation System (IVAS) and all four pillars of Army Link-16 (Ground ADA, Ground Fires, Aviation, and Gateways).
DESCRIPTION
Formally Airborne, Maritime & Fixed Station (AMF), HAMMR changed its mission by terminating the Manuever and Small Airborne Networking Radio programs to become the Army’s program for the Integrated Tactical Network (ITN), Security Forces Assistance Brigade (SFAB), and Air-Ground Networking Information System (AGNIS) missions. PM TR is also responsible for Army Link-16, HF radios, IVAS, and Combat Survivor Evader Locator radios (CSEL).

CAPABILITIES

ITN
- ITN provides a simplified, independent, mobile network solution primarily at the battalion and below level that is available down to the small-unit dismounted leader to facilitate mission command, situational awareness and air-to-ground integration.
- PM TR procures and provides interoperability tactical communication enhancement equipment, ancillaries, and related services to support ITN.
- The ITN family of radios fills critical communications gaps and includes but is not limited to High Frequency Radios; Link-16 handheld radios; line-of-sight/beyond-line-of-sight radios; foliage-dense environment radios and subterranean radios.

AGNIS
- AGNIS is a NDI multiple-channel radio that addresses multiple capability gaps within the aviation community; specifically, data communications with ground forces.
- AGNIS will support the latest released SINCGARS waveform on one channel and have the ability to host an Advanced Networking Waveform on the other channel(s), offering the users both a voice and data networking capability on Army Aviation platforms.
- AGNIS will replace the current SINCGARS ARC-201D radio on Army Aviation platforms.

Multifunctional Information Distribution Systems (MIDS)
- The MIDS (Link-16) provides multiservice/NATO interoperability and SA and supports air and missile defense engagement operations.
- Features 200-watt power amplifier enabling a range of up to 300 nautical miles
- Near real time distribution of air and missile tracks
- Nets air defense control centers
- Control air/missile defense Operations
- Secure/jam resistant communications
- High data throughput
- Time division multiple access
- 300nm (Normal)/500 nm (Extended) Range

A | American commandos during an exercise, a Special Forces soldier in Afghanistan.
B | AMF enhances situational awareness and mission command.
C | MIDS-LVT(2/11) platform-based Link 15 terminal.
WAVEFORMS

Army portable and interoperable waveforms provide mobile and ad hoc networking and network enterprise services to enhance tactical warfighting capabilities. Waveforms enable the Army’s tactical data radios to transmit voice and data across the battlespace.
PROGRAM MANAGER TACTICAL RADIO
WAVEFORMS

DESCRIPTION

Project Manager (PdM) Waveforms’ (WF) roadmap consist of two tracks:

**Track 1** is ongoing, Government/ Government Off the Shelf (GOTS) waveform business development where with continued work on DoD waveforms such as modernizing Single Channel Ground and Airborne Radio System (SINCGARS) to mitigate near-, mid-, and far-term threats; working to transition Warrior Robust Enhanced Network (WREN); and working all the Unit Task Reorganization (UTR) capabilities to ease network complexity.

**Track 2** consists of a waveform characterization strategy for commercial off-the-shelf (COTS)/Non Developmental Item (NDI) waveforms. Following the Army’s renewed interest in COTS/NDI WFS to address immediate capability gaps and growth for the Army’s tactical communications portfolio, PdM WF is implementing the COTS / NDI WF process to identify, analyze, and characterize turn-key communications products available from industry.

With this new strategy, PM TR is partnering with the Network Cross-Functional Team (N-CFT), Communications, Electronics, Research, Development and Engineering Center (CERDEC), Joint Tactical Networking Center (JTNC), and PdM Handheld/Link 16, Air to Ground, Multi Role (HAMMR) to identify promising communications and radio service solutions to make the Army’s tactical network more useable, survivable, flexible, and capable.

Solutions will be aligned to identified needs from the N-CFT and Project Manager Tactical Radios (PM TR) as the Integrated Tactical Network (ITN) Office of Primary Responsibility tracked rigorously and reported in near-real time through a collaboration tool pilot implementation (a collaboration with Joint Tactical Networking Center (JTNC), and assessed for performance and Electronic Warfare (EW) / Cyber survivability in both lab and field environments.

A | U.S. Soldiers, all assigned to B Company, 1-502nd Infantry Regiment, 2nd Brigade, 101st Airborne Division, set up AN/PRC-155 (Manpack) radios at Fort Bliss, Texas.
B | Soldier with 1st Battalion, 26th Infantry Regiment, 2nd Brigade Combat Team, 101st Airborne Division, listens on Manpack while conducting a live fire exercise.
The Tactical Network Transport at-the-halt capability provides mission command and the full range of voice, video, and data communications Soldiers and commanders need to be successful in today’s missions. This robust line-of-sight and beyond-line-of-sight network communications capability successfully meets the Army’s at-the-halt operational requirements.

• General Dynamics
• CodeMettle
• Telecommunication Systems, Inc.
• Envistacom
• Microsoft
• Riverbed Technology
DESCRIPTION
To support expanding network requirements and improve the readiness of today’s operational force, the Army continues to modernize the at-the-halt capability that increase and optimize bandwidth, improve capability and interoperability, while increasing resiliency in a contested environment. The 5th Generation Technology Insertion (5GTI) is the next effort that will refresh end-of-life (EOL) at-the-halt Tactical Network Transport equipment. The 5GTI leverages new technology and pre-existing Tactical Network products for a common user experience. It will provide more compute power, reduce size, weight and power (SWaP) and equipment setup time, while increasing usability, network resiliency and equipment flexibility.

CAPABILITIES
• The Army’s at-the-halt Tactical Network Transport has three main transportable network nodes that provide high-speed wide area network capability for secure voice, video and data exchange. The Division Hub Node (DHN) and Joint Network Node (JNN) support division headquarters; the JNN also supports brigade combat team level headquarters; and the Battalion Command Post Node (BnCPN) supports battalion level headquarters; and the Regional Hub Node (RHN), is a fixed installation equivalent to three THNs and is used to support theater level operations.
• The Satellite Transportable Terminal (STT) is a highly transportable and mobile satellite system, which operates in conjunction with the JNN and BnCPN. It is designed to establish secure voice, video and data communications virtually anytime and anywhere.

A | Soldiers from the 86th ESB help prepare the tactical network for phase three of the joint multinational JWA 18.1, in May 2018, in Germany.
B | The Army completed At-The-Halt technical refresh across the Army, which marked the Texas ARNG 36th CAB fielding marked completion, in Austin, Texas, in August 2018.
C | Thunderbirds from 62d Signal Battalion, 57th ESB, and Headquarters and Headquarters Company participate in the brigade’s field training exercise in October 2018.
Integrated on a variety of tactical vehicles to best suit unit requirements, on-the-move Tactical Network Transport configurations enable mobile mission command, secure reliable voice, video and data communications, and a real-time common operating picture from anywhere on the battlefield. On-the-move Tactical Network Transport enables Soldiers operating in remote and challenging terrain to maintain network communications while on patrol, with connectivity similar to that found in a stationary command post. Using both line-of-sight and beyond-line-of-sight for optimal network connectivity, these configurations deliver a mobile, resilient, redundant tactical communications network.

- General Dynamics
- Lockheed Martin
- L3 Technologies
- Harris Corp
- Honeywell
DESCRIPTION

On-the-move Tactical Network Transport 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/data communications using satellite based retransmission, or retrans. Retrans can be located with maneuver forces alleviating the need for isolated retrans elements that require combat power to protect.

In support of expeditionary, quick reaction and air assault mission requirements, PdM Mission Network integrated the Tactical Communications Node (TCN) and Network Operations and Security Center (NOSC) onto HMMWVs, versus Family of Medium Tactical Vehicles (FMTVs), which can be sling loaded and transported by helicopter across the battlefield or rolled onto a C-130 aircraft, making the Army more expeditionary and providing significantly increased agility and operational flexibility.

The newly fielded TCN-Lite (L); NOSC-L; Next Generation Point of Presence (NextGen PoP) and NextGen Soldier Network Extension (SNE) provide significant reductions in size, weight and power (SWaP), but more importantly, they reduce system complexity to make the systems easier to train, operate, maintain and sustain.

CAPABILITIES

• The TCN and TCN-Lite provide 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.

• The NOSC and NOSC-L provide 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 (TOC) where the communications officers manage the network. The Army plans to add the NOSC’s functions to the TCN-Lite to eliminate the need for the NOSC to reduce footprint and improve unit agility.

• The PoP and NextGen PoP 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 and NextGen PoP enable mobile mission command by providing on-the-move network connectivity, both line-of-sight and beyond-line-of-sight.

• The SNE and NextGen SNE 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.

• The Satellite Transportable Terminal (STT), a trailer-mounted ground satellite communications terminal with a generator, is used in conjunction with the TCN at the halt to provide high throughput satellite communications.
Regional Hub Nodes (RHNs) are the largest transport nodes for the Army's tactical network. The five regionally located RHNs enable global connectivity to transport information from intra-inter theater tactical networks around the world. They support current and contingency operations, humanitarian disaster relief and national emergency response.
DESCRIPTION

The five RHNs are at the uppermost level of the Army’s tactical network architecture, and their innovative baseband and satellite communications capabilities enable regionalized reach-back to the Army’s global network. They enable the transport of information across the tactical network in and out of theater and around the world. The RHNs operate out of the conflict area and give the Soldier in the field immediate access to secure and non-secure internet and voice communications anywhere on the globe. To provide tactical users with secure, reliable connectivity worldwide, the Army has positioned RHNs in five separate regions: Continental United States (CONUS) East and CONUS West, Central Command, European Command and Pacific Command.

The Global Agile Integrated Transport (GAIT) network design interconnects the RHNs -- and can also interconnect Department of Defense (DOD) Teleport Sites -- to create a global network mesh that enables high-capacity fluid data exchange from anywhere on the planet. GAIT provides more routing options, more paths and solutions for data to flow through allowing the Army to leverage the global network more efficiently and effectively. The GAIT delivers a more unified and robust network, enabling current expeditionary network capabilities and laying the ground work for future network transport innovation.

CAPABILITIES

- RHNs are currently used by both deployed Marine Corps and Army units.
- RHNs possess full Network Operations capabilities for network monitoring, management and trends analysis, as well as information assurance tools.
- RHN Commercial Internet and Phone (COM-IP) package supports contingency operations, disaster relief or U.S. homeland emergency response.
- Leveraging GAIT, commands with dispersed units around the globe can maintain mission command and Network Operations (NetOps) capabilities from their home station or forward-deployed headquarters.
- GAIT enables and enhances new capabilities, including Enroute Mission Command (EMC), Transportable Tactical Command Communications (T2C2), Modular Communications Node-Advanced Enclave (MCN-AE), Secure, Mobile, Anti-Jam, Reliable, Tactical–Terminal (SMART-T), and Disaster Incident Response Emergency Communications Terminal (DIRECT).
Enroute Mission Command (EMC) enables airborne unit commanders to plan missions in the air, while their Soldiers receive operational updates and watch full motion video of upcoming drop zones before their parachutes ever open. EMC arms Soldiers with real-time situational awareness enroute so they can be more effective the moment boots hit the ground.

- ViaSat
- Boeing
- STS
- General Dynamics
- L3 Communications
DESCRIPTION
The system’s suite of plane-to-plane, plane-to-ground network communications capabilities provide GRF 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.” EMC enables these critical early entry forces to be better prepared and to adjust their courses of action as needed prior to combating near peer adversaries on the ground.

The GRF must 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 the airborne units to access mission command capabilities, such as Command Post of the Future and secure reliable voice, video and data communications, all from an Air Force C-17 aircraft.

Because of the increased bandwidth the system provides, commanders can now tap into mission command applications and utilize services such as Secure Voice over Internet Protocol (SVoIP) phone calls, chat and email. Unmanned Aircraft System feeds can be displayed throughout the aircraft on LED screens, which also have an integrated scrolling marquee and intercom system that provides status updates.

The EMC capabilities also 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 remain synchronized.

CAPABILITIES
- The Fixed Installed Satellite Antenna (FISA) provides tactical network connectivity on an Air Force C-17 aircraft and provides a significant increase in bandwidth in flight, enabling a new host of services to be employed on board, increasing capability for units to plan and maintain critical situational awareness in the air. Once EMC’s FISA is integrated onto a C-17 aircraft, Soldiers merely roll-off the other EMC equipment, and roll it off at the end of the mission.
- 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 in which they can 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. The CASPAN has ten seat positions, four LED screens, ruggedized laptop computers, headsets, and provides adequate bandwidth to support a prioritized set of mission planning applications.
The new, easy-to-transport, high-capacity Terrestrial Transmission Line of Sight (TRILOS) Radio program-of-record will improve the expeditionary nature of U.S. Army units, while combating the increasing risk of operating its tactical network in satellite denied environments.

KEY CONTRACTORS

- Ultra, TCS
DESCRIPTION
Packed in a few rapidly deployable transit cases, the small form factor Trilos radio provides a significant reduction in size, weight and power (SWaP) compared to the current at-the-halt High Capacity Line Of Sight (HCLOS) radio, which needs two sheltered-vehicles and two large antennas to relay information. The Trilos radio increases the robustness of the Army’s tactical network by providing a significant increase in bandwidth versus the HCLOS radio, along with increased range, with lower latency than satellite communications (SATCOM).

Additionally, TRILOS is a dual channel radio as opposed to HCLOS which is a single channel radio. Thus the TRILOS radio can execute two responsibilities at the same time -- it provide point-to-point communications, but unlike the HCLOS, it will also provide point-to-multipoint communications, enabling Soldiers to shoot multiple shots with one antenna mast, versus needing extra antennas to shoot to multiple terminals. With TRILOS fewer radios, Soldiers and supporting resources are needed.

CAPABILITIES
- Significant SWaP reduction over current capability for improved unit agility
- Operates in satellite denied environments
- Significant increase in bandwidth and range vs current capability
- Easy to operate; requires only two Soldiers for set up
- Node agnostic so it can hook up to an at-the-halt Joint Network Node or Command Post Node, as well as a mobile Tactical Communications Node (TCN) or TCN-Lite
- Dual channel provides point-to-point and point-to-multipoint communications, enabling Soldiers to shoot multiple shots with one antenna mast, versus needing extra antennas to shoot to multiple terminals
- Reduces the Army’s reliance on satellites; saves significant costs by reducing the use of expensive commercial satellite airtime leases
- Adds redundancy and operational flexibility to the tactical network

A | 67th Expeditionary Signal Battalion (ESB) new equipment training and fielding for the small form factor, modular TRILOS radio and several other new expeditionary Signal Modernization capabilities in June 2018 at Fort Gordon, Georgia.
B | 67th ESB TRILOS new equipment training in June 2018 at Fort Gordon, Georgia.
C | As part of a Developmental Operations acquisition approach, PM Tactical Network tested the TRILOS radio at Fort Bliss, Texas.
The Army’s next generation Tropospheric Scatter Transmission (Tropo) capability will provide beyond-line-of-sight capability that will significantly extend network range and throughput, and greatly reduce size, weight and power (SWaP) requirements over legacy Tropo capability. The capability can also be used in satellite denied environments.
DESCRIPTION
Tropo bounces signals off of the Earth’s atmosphere to provide high-capacity beyond-line-of-sight capability without using expensive and limited satellite resources. When fielded, it will reduce the Army’s over-reliance on satellites, while saving significant costs by reducing expensive commercial satellite airtime leases. This commercial-off-the-shelf product will augment and expand the transport capacity of the Army’s tactical network.

CAPABILITIES
- Beyond-line-of-sight without satellites
- Operates in satellite denied environments
- Significant increase in bandwidth and range vs legacy Tropo capability
- Significant SWaP reduction over current capability for improved unit agility
- Reduces the Army’s reliance on satellites; saves significant costs by reducing the use of expensive commercial satellite airtime leases
- Adds redundancy and operational flexibility to the tactical network
Secure Wi-Fi uses the National Security Agency-approved Commercial Solutions for Classified solution to provide secure classified and unclassified Wi-Fi to the Command Post.
DESCRIPTION
By going wireless, Command Post setup and tear down times is significantly reduced, for increased unit maneuverability, operational flexibility, and survivability. Logistics 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. Most importantly, network downtime is significantly reduced. Following Command Post setup, units can turn on their Secure Wi-Fi hotspots and the network can come up first instead of last, in as little as minutes instead of hours, and Soldiers can stay connected longer when jumping the command post.

CAPABILITIES
- Significantly reduces Command Post setup. Eliminates 17 boxes of expensive cable weighing hundreds of pounds.
- Secure Wi-Fi 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: National Security Agency (NSA)-approved Commercial Solutions for Classified (CSfC) software based encryption
- Works with commercial, non-secure Internet Protocol Router (NIPR), secure IPR (SIPR), and coalition networks.

A | Soldiers from the 1st Armored Brigade Combat Team, 3rd Infantry Division (1/3 ID) demonstrate Secure Wi-Fi capability in the brigade main command post as part of a pilot of the capability during the unit’s training rotation at the National Training Center, at Fort Irwin, California.

B | The MA ARNG 26th MEB prepares Commercial Wi-Fi hotspot to support operations during the Vigilant Guard 19-1, in November 2018.

C | Following command post relocation, units can turn on their Secure Wi-Fi hotspot and the network can come up first instead of last.
Commercial Coalition Equipment (CCE) is packed in small form factor (SFF) transit cases and provides expeditionary coalition and commercial network connectivity to the tactical network.
DESCRIPTION
The CCE can be rapidly reconfigured to provide secure tactical access for the coalition or commercial networks to support both civil and military operations. Additionally, the CCE provides a Radio Bridging/Voice Cross-banding (RBVC) capability that enables radios on different frequencies or with different standards, or different equipment such as radios or cell phones, to seamlessly connect to each other, which is essential in both disaster response or coalition operations where different countries and organizational entities have their own equipment. The CCE can also be configured with a Commercial Radio Case (CoRC) for use in Expeditionary Signal Battalions (ESBs) or the National Guard.

Each of the coalition countries have 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. CCE enables the Army to both send and receive critical situational awareness with its coalition partners and contribute to a real-time common operating picture across the theater of operations.

CAPABILITIES
- Provides secure tactical access for coalition or commercial networks to support both civil and military operations
- CCE reduces size, weight and power (SWaP) for increased unit agility.
- CCE offers Radio Bridging Voice Cross-banding (RBVC) capability enables radios on different frequencies, or different equipment such as radios or cell phones, to seamlessly connect to each other, which is essential in both disaster response or coalition operations where different countries and organizational entities have their own equipment
- Uses the same network agnostic hardware “box” as the Modular Communications Node - Advanced Enclave (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 of the same resources they have when using the traditional standalone Trojan Intelligence Network, but instead using the Army’s Tactical Network.
DESCRIPTION

Improving the expeditionary nature of today’s force is a high priority for the Army and physical footprint is a critical factor. 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.

Additionally, unlike the intelligence network equipment, the MCN-AE 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. Compared to the Army’s intelligence network, the tactical network is more robust and redundant with multiple satellite and line-of-sight link alternatives, so it can also deliver that needed redundancy to the intelligence community. With the tactical network, if one link goes down, the network can use an alternate path to ensure that critical intelligence data gets through. Having line-of-sight options will also help enable the transfer of intelligence data in satellite denied environments.

Currently, the Army’s tactical operations, intelligence, logistics and medical communities each use separate communications networks to pass information. In the long run, the Army’s goal is to converge the intelligence, logistics and medical networks onto the tactical network, which will be conducted in a phased approach. The lightweight expeditionary MCN-AE is at the heart of the intelligence convergence effort.

CAPABILITIES

• Small form factor reduces size, weight and power (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 more robust and redundant tactical network, delivering needed redundancy to the intelligence community
• Uses the same network agnostic hardware “box” as the Commercial Coalition Equipment (CCE)
The Disaster Incident Response Emergency Communications Terminal (DIRECT) tool enables National Guard signal units to provide commercial phone, internet access, and commercial Wi-Fi and 4G LTE to first responders -- military, government and non-governmental -- during domestic natural disasters, emergencies and civil support operations.

- Janus Research
- Engineering Solutions & Products
DESCRIPTION
DIRECT securely leverages the Army National Guard’s organic satellite-based tactical network transport equipment, the same used by the Active Army, to enable voice, video and data communications, even when local infrastructure has been damaged or destroyed. The DIRECT tool suite also comes with a voice bridging capability that connects disparate radios operating on different frequencies, and it interconnects military and first responder radios, cell phones and internet telephones, to enable a seamless collaboration and synchronization across the entire team.

DIRECT is replacing the Army National Guard’s legacy Joint Incident Site Communication Capability (JISCC). Although JISCC aided first responder communications, it did not enable the military and first responders to directly communicate over the robust tactical network. Since DIRECT falls under an Army program, training and sustainment are built into the capability, enabling the Guard to operate, manage and maintain the equipment more easily and cost effectively compared to the previous capability. DIRECT will be fielded to all 50 states and four territories with an Army National Guard presence.

CAPABILITIES
• The Joint Network Node (JNN) is organic to the unit and is also the same system used by Active Army units. This transportable network node provides high-speed wide area network capability for secure voice, video and data exchange.
• The Satellite Transportable Terminal (STT) is also organic to the unit and used by Active Army units. This highly transportable and mobile satellite system operates in conjunction with the JNN and is designed to establish secure voice, video and data communications virtually anytime and anywhere, even if local infrastructure has been destroyed.
• Commercial Coalition Equipment (CCE), the same used by the Active Army, fits into a single man-portable transit case and provides the tactical access to commercial internet and tele- phone services. Integrated into the CCE, the radio-bridging and voice cross-banding capability enables interconnection between cell, landline and Voice over Internet Protocol (VoIP) calls, and various military and first responder radios. It enables seamless interoperability among disparate radio networks without supplying common radios to all the users, as was done in the past. Army National Guardsmen can combine radio and phone networks for crossed communications or create secure forums where various agencies can talk in independent groups.
• Commercial Wi-Fi and Commercial 4G LTE Cellular capability will support Soldier wireless and cellular handheld requirements. The Commercial Wi-Fi capability covers a limited footprint and is used inside the ‘skin’ of the incident site tent, while 4G LTE is used with smartphones and eventually tablets to extend coverage to an entire base radius.
• The DIRECT package also includes a towed generator, towed equipment trailer with communications equipment, tent and support supplies.

A | The North Carolina Army National Guard used its DIRECT tactical network communication tool suite to provide lifesaving communications capabilities to first responders in the area. (U.S. Army National Guard Photo by Sgt. Devon Bistarkey)
B | MA ARNG 26th MEB erects an antenna, part of its DIRECT equipment tool suite, during the Vigilant Guard 19-1 at Gillette Stadium, in November 2018.
C | MA ARNG 26th MEB sets up a Wi-Fi antenna to support operations during the Vigilant Guard 19-1 at the Charlemon Fairgrounds in November 2018.
Area Common User System Modernization (ACUS MOD) program provides planned network upgrades through technology insertions into the current force to support the Army’s current on-the-move Tactical Network Transport force modernization efforts. It includes increased network services and management, information assurance, enhanced reach-back and increased transport speed and bandwidth required to support the Soldier’s increasing need for high-speed data, voice, video and imagery through the recapitalization of current force systems.

- General Dynamics
- CACI
- Engineering Solutions & Products
- Janus Research
DESCRIPTION

ACUS MOD provides Internet network management capabilities, as well as integrated voice, video and data services. It also provides for beyond-line-of-sight (BLOS) transmission capability. ACUS MOD provides increased situational awareness to unit commanders, improved throughput and joint and coalition interoperability at battalion and above. It also implements commercial-based technology insertions into the current force for smooth technology upgrades.

CAPABILITIES

- Battlefield Video Tele-Conferencing (BVTC) III provides commanders with access to accurate, timely situational information and is interoperable with the existing communication Local Area Network (LAN) infrastructure across a multi-platform backbone network. It assists commanders in coordinating and interacting with different echelons and adjacent units. BVTC III replaces the antiquated BVTC II system and significantly increases system power, simplicity, and capability, while reducing size, weight and power requirements (SWaP).

- Tactical Network Operation (NetOps) Management System (TNMS) is a scalable modular NetOps capability that enables signal Soldiers to plan, configure, manage, monitor, control and secure/defend their tactical network assets. TNMS is fielded to units that are not provided with traditional Tactical Network Transport NetOps capabilities. The TNMS Planner capability enables Soldiers to map out the most effective strategic locations to place radios and to position the antennas for the most effective links before they even reach the battlefield. The TNMS will facilitate decision-making necessary to quickly identify network problems, shift resources, change configurations and coordinate the management of the critical network infrastructure supporting mission command functions.
  - The Single Shelter Switch (SSS), designed for rapid deployment and small footprint, provides “first in” capability and a building block for network expansion. The SSS has been enhanced to provide joint and coalition interoperability with commercial-off-the-shelf and government-off-the-shelf technologies for continued upgrade ease. The SSS provides communication officers (S6s) increased functionality in a single vehicle shelter.
  - The legacy AN/TRC-190 High Capacity Line Of Sight (HCLOS) radio provides the line-of-sight capability for at-the-halt Tactical Network Transport. The Army is replacing the HCLOS radio with the new small form factor Terrestrial Transmission (Trilos) Radio. Trilos is packed in a few rapidly deployable transit cases, and will provide a significant reduction in size, weight and power (SWaP) with increased range and bandwidth.
  - The legacy AN/TRA-170(V)3 Tropospheric Scatter Transmission (Tropo) system, provides beyond-line-of-sight communications to extend the tactical mission command network. The next generation Tropospheric Scatter Transmission (Tropo) capability will provide beyond-line-of-sight capability that will significantly extend network range and throughput, and greatly reduce size, weight and power (SWaP) requirements over the legacy Tropo.
The air-jumpable Transportable Tactical Command Communications (T2C2) Lite and the T2C2 Heavy high-bandwidth satellite terminals will enable initial entry forces to connect to the Army’s tactical and strategic network to obtain the situational awareness and mission command capabilities needed to conduct initial entry operations and set the stage for follow-on forces. In more mature operations, T2C2 Heavy will provide high bandwidth tactical network extension to company level and small forward operating bases and T2C2 Lite will support special teams in austere locations with high bandwidth requirements.
DESCRIPTION
T2C2 provides satellite capability to small detachments and teams operating in remote locations without network infrastructure, enabling them to securely relay critical and time sensitive information, increasing the situational awareness for the entire operation. T2C2 greatly increases throughput over currently fielded systems by taking advantage of military satellite capability. Because the T2C2 solution is inflatable, it can provide a larger dish size, with increased capability and bandwidth efficiency, in a smaller transportable package. These highly expeditionary inflatable satellite antennas provide the commander with increased operational flexibility and speed in maneuver.

Until T2C2 fielding is complete, Secure Internet Protocol Router Network/Non-Secure Internet Protocol Router (SIPR/NIPR) Access Points (SNAPs) and even smaller suitcase-sized Global Rapid Response Information Packages (GRRIPs), are being used as bridging capability.

CAPABILITIES
T2C2 Lite (AN/TSC-232) 1.2M: X-Band
- Transportable by two-man team with rapid setup
- Supports two user defined enclaves: (NIPR/SIPR/Coalition Secret) and a Colorless Core enclave
- Three user access ports per user enclave

T2C2 Heavy (AN/TSC-233) 2.4M: Ka-Band
- Transportable in five hard sided transit cases
- Supports three user defined enclaves (NIPR/SIPR/Coalition Secret) and a Colorless Core enclave
- 16 user access ports per user enclave

A | 3rd BCT, 82nd ABN Div T2C2 new equipment training (the first unit equipped), in February and March 2018, at Fort Bragg, North Carolina.
B | The 2nd BCT, 10th MTN Div used its Heavy and Lite T2C2 systems during its training rotation at the JRTC in Fort Polk, Louisiana, in June 2018.
C | The 2nd SFAB T2C2 new equipment training in September 2018, at Fort Bragg, North Carolina.
The Scout satellite terminal [or micro Very Small Aperture Terminal (micro-VSAT)] provides expeditionary satellite communications in remote locations. This non-program of record system can be used by a single general purpose user and sets up rapidly. Packing options include small backpacks, a single commercial aircraft overhead transit case and soft side roll aboard luggage.
DESCRIPTION
The Scouts provide small teams with an expeditionary satellite capability for low bandwidth communications and exchange of secure and non-secure data, voice, and video.

CAPABILITIES
• Major system components have been modularized into separable subsystems to meet customer needs and to simplify upgrades and logistics
• Can be configured for single, dual or tri-band operation at time of delivery or through field upgrades
• Rapid setup/teardown by one General Purpose User
• Packaging options include small backpacks, a single-commercial aircraft compliant overhead transit case and soft side roll aboard luggage
• Terminal operators can change frequency bands in the field without tools
• Three variants: V1-65cm Dish; V2-95cm Dish; V3-1.3m Dish

A | Soldiers from the 50th Expeditionary Signal Battalion-Enhanced (ESB-E) tear down a Scout satellite dish during a demonstration for the XVIII Airborne Corps deputy commander, on Nov. 29, 2018, at Fort Bragg, NC.
B | Soldiers from the 50th ESB-E tear down a Scout satellite dish during a demonstration for the XVIII Airborne Corps deputy commander, on Nov. 29, 2018, at Fort Bragg, NC.
C | The 50th ESB-E used this Scout satellite terminal to provide network comms to the 108th ADA Brigade command post, during a field exercise, at Fort Bragg, NC, in November 2018.
Fitting into a single handheld 28 pound transit case for rapid mobility, the satellite network communications kit known as the Global Rapid Response Information Package (GRRIP) provides secure, beyond-line-of-sight voice, and data communications without the need for local network infrastructure, so Soldiers can communicate anytime and anywhere on the planet.
DESCRIPTION
The GRRIP is small enough to fit into the overhead bin of commercial aircraft and sets up rapidly. The system provides access to Defense Information Systems Network (DISN) services, which enables initial entry elements to transfer critical information (data/voice) to commanders. GRRIP provides classified and unclassified communications to forces operating in austere and demanding environments, who do not have access to the network equipment and infrastructure of established forward operating bases. This commercial off-the-shelf terminal is designed for small teams entering locations where the infrastructure has either been dismantled, destroyed or is non-existent.

CAPABILITIES
• Network communications from anywhere on the planet with no reconfiguration and uses L-Band based satellite access
• Fits into a single handheld transit case for rapid mobility and force scalability
• Continued communications and situational awareness from early entry to the tactical edge in more mature operations
• Can be configured for use on Secure Internet Protocol Router Network (SIPR) Non-Secure Internet Protocol Router (NIPR) or coalition networks

A | GRRIP enables the Soldier or first responder to communicate anywhere in the world by using SIPR/NIPR or coalition voice and data capability without electricity or an existing infrastructure.
B | Soldiers from the Army’s 20th Chemical, Biological, Radiological, Nuclear, Explosives (CBRNE) Command connect an extra laptop into the GRRIP so they can work on both NIPR and classified SIPR networks simultaneously.
C | GRRIPs provide secure and non-secure communications to forces operating in austere and demanding environments such as embedded training teams and other small units that do not have access to the network equipment and infrastructure of established forward operating bases.
The Secure, Mobile, Anti-Jam, Reliable, Tactical–Terminal (SMART-T) is the Army’s protected satellite communications system that enables commanders at brigade and higher to operate in an electronic warfare (EW) threat environment that includes both radio frequency signal interference (jamming), signal detection and geographic location threats.
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 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.

CAPABILITIES
• Interoperable with AEHF satellite constellation
• Enhanced system interfaces
• Provides Low and Medium Data Rate (LDR/MDR) or Extreme Data Rate (XDR) capability for voice and data transmission
• Interoperable with MILSTAR, EHF MIL-STD 1582D and MIL-STD 188-136 compatible payloads
• Provides anti-jam and anti-scintillation (nuclear environment) communications

A | The 2nd BCT, 1st ID used this SMART-T at Hohenfels Training Area, Germany, January 25, 2018, during Allied Spirit VIII.
B | The 3rd BCT, 82nd ABN Div used this SMART-T during NIE 18.2 at Fort Bliss, Texas in November 2018.
C | The 2nd BCT, 101st ABN Div used these SMART-Ts on March 20, 2018, during its JRTC rotation, at Fort Polk, Louisiana.
Phoenix terminals provide Expeditionary Signal Battalions (ESBs) with high capacity, inter- and intra-theater range extension for networked battle command and control information, including logistical, operational, intelligence, and administrative data.
DESCRIPTION
The Phoenix terminal is a transportable, quad-band, tactical satellite terminal that is mounted on an expanded capacity vehicle. It provides ESBs assured access to satellite communications and operational flexibility in a tactical environment by providing a rapidly deployable capability to operate over military X/Ka and commercial C/Ku satellite bands. It is designed to operate 24 hours per day, seven days per week and provides reliable communications throughout the world.

CAPABILITIES
• Operates in military X and Ka band and commercial C and Ku bands
• Qualified for the military environment: temperature, shock, vibration
• Can interface with other strategic networks via standardized tactical entry points, Regional Hub Nodes or strategic assets
• Transmits one Frequency Division Multiple Access (FDMA) link and receives up to four FDMA links simultaneously
• Multi-carrier capable (transmit two FDMA carriers) in C, Ku and Ka band
• Supports point to point, mesh and hub-spoke networks

A | On May 1, 2018, the 86th ESB helped prepare the tactical network for phase three of the joint multinational JWA 18.1 in Germany.
B | The U.S. 44th ESB, 2nd TTSB used this Phoenix terminal during exercise Allied Spirit VIII, Jan. 31, 2018 in the Hohenfels Training Area, Germany. (Photo Credit: Mr. William B King, 2nd Signal Brigade)
Global Broadcast Service (GBS) provides real-time situational awareness to commanders and Soldiers and can be used to inform and update disadvantaged units on the battlefield that are disconnected from the tactical network.
DESCRIPTION
GBS provides receive-only high-speed broadcast of large-volume data and multimedia products including Unmanned Aerial Vehicle (UAV) video, imagery, intelligence, maps, weather, biometric data, and security and system software updates, to deployed command posts and garrisoned forces worldwide.

GBS consists of a variety of receive suites that are owned and operated by the armed services and other government agencies, and a Satellite Broadcast Manager (SBM) co-located with Defense Information System’s Agency’s (DISA) Defense Enterprise Computing Centers (DECC). The DECC SBM connects to a variety of national sources through the DoDIN and generates broadcasts for transmission over Wideband Global SATCOM (WGS) satellites through worldwide DoD Teleport/Standard Tactical Entry Point (STEP) sites.

CAPABILITIES
- Provides near real-time situational awareness to commanders and Soldiers
- Operates over the WGS system, augmented as required by commercial Ku band satellites
- Reduces burden on the Tactical Network: By leveraging Department of Defense (DOD) Information Network (DoDIN), network and satellite constellation bandwidth demands are reduced thus, providing more satellite/network bandwidth to deployed forces
- Receives data at a rate 20 times higher than current tactical network ground terminals
- Easy to deploy Ground Receive Suites enables deployed forces to directly receive two channels of national level data and full motion video and distribute to them to command post local area network users.

A | GBS new equipment training with the 2nd Brigade Combat Team, 1st Cavalry Division at Fort Hood, Texas, in July 2018.
B | Soldier from the Penn. ARNG 2nd BCT, 28th ID connects the antenna during a test using GBS to deliver software upgrades at the unit’s armory in Washington, Pennsylvania.
C | GBS new equipment training with the 2nd Brigade Combat Team, 1st Cavalry Division at Fort Hood, Texas, in July 2018.
Deployable Ku band Earth Terminals (DKETs) are non-program of record systems used at brigade and higher headquarters elements to augment the Army’s tactical communications network infrastructure. 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.

- Datapath
- General Dynamics
DESCRIPTION
The DKET reduces the traffic load on the Army’s five worldwide Regional Hub Nodes by providing network hub services for disadvantaged forward operating bases.
DKETs are satellite terminals designed for use at larger hub locations. They support commercial Ku-band frequencies, and have been certified for Ka and X band capability to take advantage of U.S. military satellites. They are transportable and self-contained, and can establish headquarters-level, network-hub connectivity anywhere a mission dictates.

CAPABILITIES
• DKETs are currently deployed in three configurations: Light (3.7 – 3.9M), Mobile (4.5M) and standard (4.6M – 7M), with the majority being the light design. This lighter design 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.
• DKETs operate on Ku, Ka and X-band frequencies.
• Electronics are housed in separate shelters

A | 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 | A DKET is shown in March 2011 as part of Project Manager Tactical Network’s Ka and X-band frequency certification effort that enables earth satellite terminals to utilize military satellites.
Secure Internet Protocol Router/Non-Secure Internet Protocol Router (SIPR/NIPR) Access Point (SNAP) ground satellite terminals are fielded to augment current tactical network capabilities to extend network access to forward operating bases (FOBs) at the company, platoon and team level.
DESCRIPTION
This non-program of record system bridges gaps in C4ISR created by rugged and expansive terrain and sparse infrastructure. SNAPs provide access to the tactical network (SIPR, NIPR, and Coalition networks), enabling mission command, information exchange (voice, video and data), call for fires and Medevac support. SNAPs are a key communications component for smaller units, providing secure beyond-line-of-sight communications and network connectivity.
These commercial-off-the-shelf Very Small Aperture Terminal (VSAT) satellite terminals can deploy more quickly than larger satellite terminals. The transit case design enables easy transport in the back of High Mobility Multipurpose Wheeled Vehicles or helicopters, and the modular design allows for varying dish and antenna sizes to appropriately satisfy mission requirements.

CAPABILITIES
• Provides robust, long-range, beyond-line-of-site SIPR, NIPR and Coalition network communications capability down to the tactical company, platoon or team FOB.
• Interoperable with both the at-the-halt and on-the-move tactical network equipment, as part of the tactical network architecture.
• Transit case design enables easy transport in the back of High Mobility Multipurpose Wheeled Vehicles or helicopters.
• Modular design allows for varying dish and antenna sizes to appropriately satisfy mission requirements.
• Easy to move around the battlefield, providing an expeditionary element to the force.
• Certified Ka and X-band capability to take advantage of the Department of Defense’s Wideband Global SATCOM satellites.

A | Soldiers of the Florida National Guard’s 146th Expeditionary prepare their SNAP terminals for deployment to support military and civilian communications during Hurricane Irma.
B | Soldiers hook up wires to SNAP terminals during exercises at Fort Hood, Texas in September 2018. The training they will receive will help the U.S. Army provide communication stateside and during theater operations.
Unified Network Operations (UNO) provides an integrated, standardized, and simplified “NetOps framework” that will combine the management of the strategic and tactical network environments into an Army centrally integrated NetOps architecture.
DESCRIPTION
The program delivers a robust, integrated, standardized set of network management capabilities that enable communications officers (S6/G6) from tactical edge up through corps to plan, configure, manage, monitor, control and secure/defend their network assets. UNO efforts simplify and reduce the number of network management tools communication officers (G6s and S6s) use to manage and defend the tactical communications network and the program leads the Army’s Tactical NetOps convergence efforts. UNO assures uninterrupted access to critical communications and information links [satellite communications, positioning, navigation, and timing (PNT), and intelligence, surveillance, and reconnaissance (ISR)] across a multi-domain architecture, even when operating in a contested, congested, and competitive operating environment.
UNO integrates network management capability to simplify user experience, increase situational awareness, strengthen Cyber Network Defense capability, and integrate network planning with mission planning capabilities. It delivers capability as software upgrades that run in multiple common operating environment (COE) computing environments. Additionally, the program integrates functionality between the tools of the Upper Tactical Internet and Lower Tactical Internet, enhances visualization of NetOps functions and pushes network data to cyber situational awareness tools. UNO also implements a common data model that enables reconfiguration of the Network in support of unit task reorganization.

CAPABILITIES
• Delivers advancements in the monitoring, control and planning tools to simplify management of emerging voice, data and internet transport networks
• Modeling and simulation capability to analyze the best possible network configuration with dynamically changing network due to global complex variants
• Provides improved information assurance and Network Centric Enterprise Services
• Inherent software modernization through recurring technical refresh within the PM Tactical Network family of programs
• Provides NetOps users with the capability to “operationalize” the planning, configuration, monitoring and management of the network through a single consistent tailor-able user interface
• COE compliant, portable, and interactive common GUI with a user definable presentation workspace/dashboard
• Integrates network planning with mission planning, enabling the S6 to optimize capability to move data around the virtual battlefield in support of the Commander’s scheme of maneuver
• Integrates Upper Tactical Internet and Lower Tactical Internet network management tools and services
• Provides near-term “bridging” of NetOps capabilities for tactical radios and tactical network transmission systems operating within the tactical environment
• Sets the foundation for further integration of tactical and strategic networks for both network management services and cyberspace operations
The Joint Enterprise Network Manager (JENM) is a consolidated software application that plans, loads, manages and secures/defends mid and lower-tier software defined radios and associated waveforms, including: the Mobile User Objective System (MUOS), as well as the Single Channel Ground and Airborne Radio System (SINCGARS) and some Satellite Communications.
DESCRIPTION
JENM can plan and configure an entire network of disparate networking radios and waveforms, ensuring interoperability across and between echelons. Its new enterprise Over-the-Air Management (eOTAM) capability reduces manpower hours to reconfigure, manage, control a tactical radio network, by performing the tasks rapidly over-the-air. The JENM eOTAM capability reduces the need for Signal Soldiers to travel from location to location, allowing them to manage and configure their radio networks from remote locations, such as the battalion tactical operations cell. Additional improvements to JENM include a more intuitive graphical user interface, simplification in planning tactical networks, network monitoring and troubleshooting, and capability with more software defined radios and respective waveforms.

New JENM enhancements are also helping pave the way for the convergence of NetOps tools and management for both the Upper Tactical Internet and the Mid and Lower Tactical Internet (radio networks). The goal of NetOps convergence is to provide one framework for integration of tools into a single seamless delivery so that the S6 has one tool set to more easily see and manage the entirety of the network. The S6 will be able to see all the many facets of the network in one cohesive picture.

The Joint Tactical Network Environment Network Operations Toolkit (J-TNT) consolidates separate lower tactical network tools onto a single laptop to streamline how signal Soldiers manage the tactical network. J-TNT will host three software applications: JENM, Coalition Joint Spectrum Management Planning Tool (CJSMPPT) and Systems Planning Engineering and Evaluation Device (SPEED). J-TNT will be integrated into the core tactical network capability baseline software and it will remain a standalone platform for units with Software Defined Radios and without direct tactical network connectivity.

CAPABILITIES
• Operates within the Integrated Tactical Networking Environment and handles the planning, configuration, monitoring, management, and analysis functions for all signal components and systems within the Joint tactical radio environment.
• Reduces manpower hours to reconfigure, manage, and control a tactical radio network, by performing the tasks rapidly over-the-air.
• Paves the way for the convergence of NetOps tools and management for both the Upper Tactical Internet and the Mid and Lower Tactical Internet (radio networks).
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>KEN</td>
<td>Key Leader Enroute Node</td>
</tr>
<tr>
<td>KMI</td>
<td>Key Management Infrastructure</td>
</tr>
<tr>
<td>LDIF</td>
<td>Lightweight Directory Interchange Format</td>
</tr>
<tr>
<td>LFED</td>
<td>Lightweight Forward Entry Device</td>
</tr>
<tr>
<td>LOS</td>
<td>Line Of Sight</td>
</tr>
<tr>
<td>LUT</td>
<td>Limited User’s Test</td>
</tr>
<tr>
<td>LANs</td>
<td>Local Area Networks</td>
</tr>
<tr>
<td>LDR</td>
<td>Low Data Rate</td>
</tr>
<tr>
<td>MDR</td>
<td>Medium Data Rate</td>
</tr>
<tr>
<td>LRIP</td>
<td>Low Rate Initial Production</td>
</tr>
<tr>
<td>MGC</td>
<td>Management Client</td>
</tr>
<tr>
<td>MP</td>
<td>Manpack</td>
</tr>
<tr>
<td>MIRARS</td>
<td>Manpower Information Retrieval and Reporting System</td>
</tr>
<tr>
<td>MNVR</td>
<td>Mid-tier Networking Vehicular Radios</td>
</tr>
<tr>
<td>MIL-STD</td>
<td>Military Standard</td>
</tr>
<tr>
<td>MRAPs</td>
<td>Mine-Resistant Ambush Protected</td>
</tr>
<tr>
<td>MC</td>
<td>Mission Command</td>
</tr>
<tr>
<td>MUOS</td>
<td>Mobile User Objective System</td>
</tr>
<tr>
<td>MTOE</td>
<td>Modification Table of Organization and Equipment</td>
</tr>
<tr>
<td>MCN-AE</td>
<td>Modular Communications Node - Advanced Enclave</td>
</tr>
<tr>
<td>MCE</td>
<td>Mounted Computing Environment</td>
</tr>
<tr>
<td>MFoCS</td>
<td>Mounted Family of Computer Systems</td>
</tr>
<tr>
<td>MIDS</td>
<td>Multifunction Information Distribution System</td>
</tr>
<tr>
<td>NSA</td>
<td>National Security Agency’s</td>
</tr>
<tr>
<td>NBOI</td>
<td>Network Basis of Issue</td>
</tr>
<tr>
<td>NetOps</td>
<td>Network Operations</td>
</tr>
<tr>
<td>NOSC-L</td>
<td>Next Generation Load Device</td>
</tr>
<tr>
<td>NVD</td>
<td>Night Vision Device</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>OTM</td>
<td>On-The-Move</td>
</tr>
<tr>
<td>PFED</td>
<td>Pocket-Sized Forward Entry Device</td>
</tr>
<tr>
<td>PoP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>PF-D</td>
<td>Precision-Fires Dismounted</td>
</tr>
<tr>
<td>PEOS</td>
<td>Program Executive Office Command, Control and Communication-Tactical</td>
</tr>
<tr>
<td>PMO Net E</td>
<td>Program Management Office Network Enablers</td>
</tr>
<tr>
<td>PM MC</td>
<td>Project Manager Mission Command</td>
</tr>
<tr>
<td>PM TR</td>
<td>Project Manager Tactical Radios</td>
</tr>
<tr>
<td>PM TN</td>
<td>Project Manager Tactical Network</td>
</tr>
<tr>
<td>PoR</td>
<td>Program of Record</td>
</tr>
<tr>
<td>PA</td>
<td>Public Affairs</td>
</tr>
<tr>
<td>RBVC</td>
<td>Radio Bridging Voice Cross-banding</td>
</tr>
<tr>
<td>ROMO</td>
<td>Range of Military Operations</td>
</tr>
<tr>
<td>RHN</td>
<td>Regional Hub Nodes</td>
</tr>
<tr>
<td>RDPs</td>
<td>Remote Desktop Protocols</td>
</tr>
<tr>
<td>RR</td>
<td>Rifleman Radio</td>
</tr>
<tr>
<td>SBM</td>
<td>Satellite Broadcast Manager</td>
</tr>
<tr>
<td>SATCOM</td>
<td>Satellite Communications</td>
</tr>
<tr>
<td>SSM</td>
<td>Satellite Transferable Terminal</td>
</tr>
<tr>
<td>STT</td>
<td>Satellite Transferable Terminal Plus</td>
</tr>
<tr>
<td>STT+</td>
<td>Satellite Transferable Terminal Plus</td>
</tr>
<tr>
<td>SOTM</td>
<td>Satellite On-The-Move</td>
</tr>
<tr>
<td>SHIELD</td>
<td>Secure High Assurance Inline Encryption Link Device</td>
</tr>
<tr>
<td>SIPR</td>
<td>Secure Internet Protocol Router</td>
</tr>
<tr>
<td>SIPRNET</td>
<td>Secure Internet Protocol Router Network</td>
</tr>
<tr>
<td>SMART-T</td>
<td>Secure, Mobile, Anti-Jam, Reliable, Tactical - Terminal</td>
</tr>
<tr>
<td>SIMCI</td>
<td>Simulation to Mission Command Interoperability</td>
</tr>
<tr>
<td>SINCGARS</td>
<td>Single Channel Ground Airborne Radio System</td>
</tr>
<tr>
<td>SIF</td>
<td>Single Interface to the Field</td>
</tr>
<tr>
<td>SSS</td>
<td>Single Shelter Switch</td>
</tr>
<tr>
<td>SKL</td>
<td>Simple Key Loader</td>
</tr>
<tr>
<td>SNAP</td>
<td>SIPR/NIPR Access Points</td>
</tr>
<tr>
<td>SA</td>
<td>Situational Awareness</td>
</tr>
<tr>
<td>SCA</td>
<td>Software Communications Architecture</td>
</tr>
<tr>
<td>SCA</td>
<td>Software Development Kit</td>
</tr>
<tr>
<td>SNE</td>
<td>Soldier Network Extension</td>
</tr>
<tr>
<td>SRW</td>
<td>Soldier Radio Waveform</td>
</tr>
<tr>
<td>SWaP</td>
<td>Size, Weight and Power</td>
</tr>
<tr>
<td>SPIR</td>
<td>Special Purpose Integrated Remote Intelligence Terminal</td>
</tr>
<tr>
<td>SOTM</td>
<td>Satellite On-The-Move</td>
</tr>
<tr>
<td>STEP</td>
<td>Standard Tactical Entry Point</td>
</tr>
<tr>
<td>SMC</td>
<td>Strategic Mission Command</td>
</tr>
<tr>
<td>SHF</td>
<td>Super High Frequency</td>
</tr>
<tr>
<td>SNC</td>
<td>Systems Planning Engineering and Evaluation Device</td>
</tr>
<tr>
<td>TCG</td>
<td>Tactical Communication Node</td>
</tr>
<tr>
<td>TCN-L</td>
<td>Tactical Communication Node-Lite</td>
</tr>
<tr>
<td>TDI</td>
<td>Tactical Defensive Infrastructure</td>
</tr>
<tr>
<td>TDM</td>
<td>Tactical Digital Media</td>
</tr>
<tr>
<td>TGR</td>
<td>Tactical Ground Reporting</td>
</tr>
<tr>
<td>THN</td>
<td>Tactical Hub Node</td>
</tr>
<tr>
<td>TI</td>
<td>Tactical Internet</td>
</tr>
<tr>
<td>TMAK</td>
<td>Tactical Media Acquisition Kit</td>
</tr>
<tr>
<td>TMC</td>
<td>Tactical Mission Command</td>
</tr>
<tr>
<td>TNIC</td>
<td>Tactical Network Initialization &amp; Configuration</td>
</tr>
<tr>
<td>TNMS</td>
<td>Tactical Network Operation Management System</td>
</tr>
<tr>
<td>TOC</td>
<td>Tactical Operation Center</td>
</tr>
<tr>
<td>TRR</td>
<td>Tactical Radio Report</td>
</tr>
<tr>
<td>TSI</td>
<td>Tactical Server Infrastructure</td>
</tr>
<tr>
<td>UHF</td>
<td>Ultra High Frequency</td>
</tr>
<tr>
<td>UNO</td>
<td>Unified Network Operations</td>
</tr>
<tr>
<td>UTTS</td>
<td>Unified Trouble Ticketing System</td>
</tr>
<tr>
<td>URN</td>
<td>Unit Reference File</td>
</tr>
<tr>
<td>USF</td>
<td>Unit Set Fielding</td>
</tr>
<tr>
<td>UTO</td>
<td>Unit Task Organization</td>
</tr>
<tr>
<td>UTR</td>
<td>Unit Task Reorganization</td>
</tr>
<tr>
<td>USMTF</td>
<td>United States Message Text Format</td>
</tr>
<tr>
<td>UAS</td>
<td>Unmanned Aircraft System</td>
</tr>
<tr>
<td>VHF</td>
<td>Variable Message Format</td>
</tr>
<tr>
<td>C4ISR/EW</td>
<td>Vehicle Integration for C4ISR/EW Interoperability</td>
</tr>
<tr>
<td>VWP</td>
<td>Vehicle Wireless Package</td>
</tr>
<tr>
<td>VSAT</td>
<td>Very Small Aperture Terminal</td>
</tr>
<tr>
<td>VM</td>
<td>Virtual Machine</td>
</tr>
<tr>
<td>VoIP</td>
<td>Voice over Internet Protocol</td>
</tr>
<tr>
<td>WGS</td>
<td>Wideband Global SATCOM</td>
</tr>
<tr>
<td>WNW</td>
<td>Wideband Networking Waveform</td>
</tr>
<tr>
<td>WCPs</td>
<td>Wireless Communications Products</td>
</tr>
<tr>
<td>WIN-T</td>
<td>Warfighter Information Network-Tactical</td>
</tr>
<tr>
<td>WIT</td>
<td>Warfighter Initialization Tool</td>
</tr>
</tbody>
</table>
FOR MORE INFORMATION

PUBLIC SITE: HTTP://PEOC3T.ARMY.MIL
FACEBOOK: HTTP://WWW.FACEBOOK.COM/PEOC3T
TWITTER: HTTP://TWITTER.COM/PEOC3T
FLICKR: HTTPS://WWW.FLICKR.COM/PHOTOS/PEOC3TMEDIA