C3 COMMAND, CONTROL, AND COMMUNICATIONS

Modernization Strategy

SEPTEMBER 2020

This page intentionally left blank.

Foreword

Command, control, and communications (C3) systems are fundamental to all military operations, delivering the critical information necessary to plan, coordinate, and control forces and operations across the full range of Department of Defense (DoD) missions. Historically, the U.S. military achieved and maintained a dominant C3 technological advantage but peer competitors and adversaries have closed the gap. DoD's current C3 systems are not keeping pace with the threat or meeting our Joint Warfighters' ever increasing information exchange needs. The Joint Force must be equipped with the latest C3 capabilities providing real-time situation awareness and decision support across all domains.

Future conflicts could well be decided by information advantage, success going to the side that transforms vast amounts of data from distributed sensors and weapons systems across multiple domains into actionable information for better, faster decision making and precision effects. The Department is executing a focused effort to realize agile and resilient command and control (C2) rapidly across all domains through integrated and synchronized capability development to ensure operational and competitive advantage over our adversaries. This effort, referred to as joint all-domain command and control (JADC2), is the art and science of decision-making to translate decisions rapidly into action, leveraging capabilities across all domains and with mission partners to achieve operational and information advantage in both competition and conflict. JADC2 requires new concepts, science and technology, experimentation, and sustained investment over many years.

This strategy represents the Department's vision for implementing the C3 portion of the *DoD Digital Modernization Strategy* and provides direction for bridging the gap between today's legacy C3 enabling capabilities and JADC2. It describes how the Department will innovate for competitive advantage while building the foundation for a fully networked communications transport layer and advanced C2 enabling capabilities to synchronize joint all-domain operations against 21st century threats. The strategy focuses on protecting and preserving current C3 capabilities; ensuring reliable U.S., ally, and key partner access to critical information at time of need; and providing seamless, resilient, and secure C3 transport infrastructure enabling a more lethal Joint Force across the full range of military operations. Implementation of this strategy requires synchronizing near-term modernization efforts in and across operating domains, transitioning from stove-piped solutions to a highly connected, agile, and resilient system.

The goals established in this document provide clear guidance and direction to modernize the Department's C3 systems and infrastructure. Modernization is not an end, however, but a continuous undertaking. DoD will assess and update the strategy to adapt to new concepts of operations and technologies on the road to JADC2.

David L. Norquist
Deputy Secretary of Defense

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

Introduction

DoD is confronting the most complex and competitive global security environment in decades. In this new era of great power competition, the Department must increase lethality for the Joint Warfighter, strengthen partnerships and alliances and attract new partners, and reform DoD for greater performance and affordability.

As we build a more lethal force and strengthen alliances and partnerships, the Department must focus on the critical enabling tools to employ the Joint, Multinational Force effectively against great power competition. Effective force employment begins with effective C2, the exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. In modern warfare this may be human-to-human, machine-to-machine (M2M) with a human in the loop, or, with increasing levels of autonomy, M2M with a human on the loop. At its most basic level, successful C2 requires assured communications, the means of sending and receiving information, and other enabling capabilities to process and display actionable information to aid commanders in the decision making process and achieve a decisive information advantage.

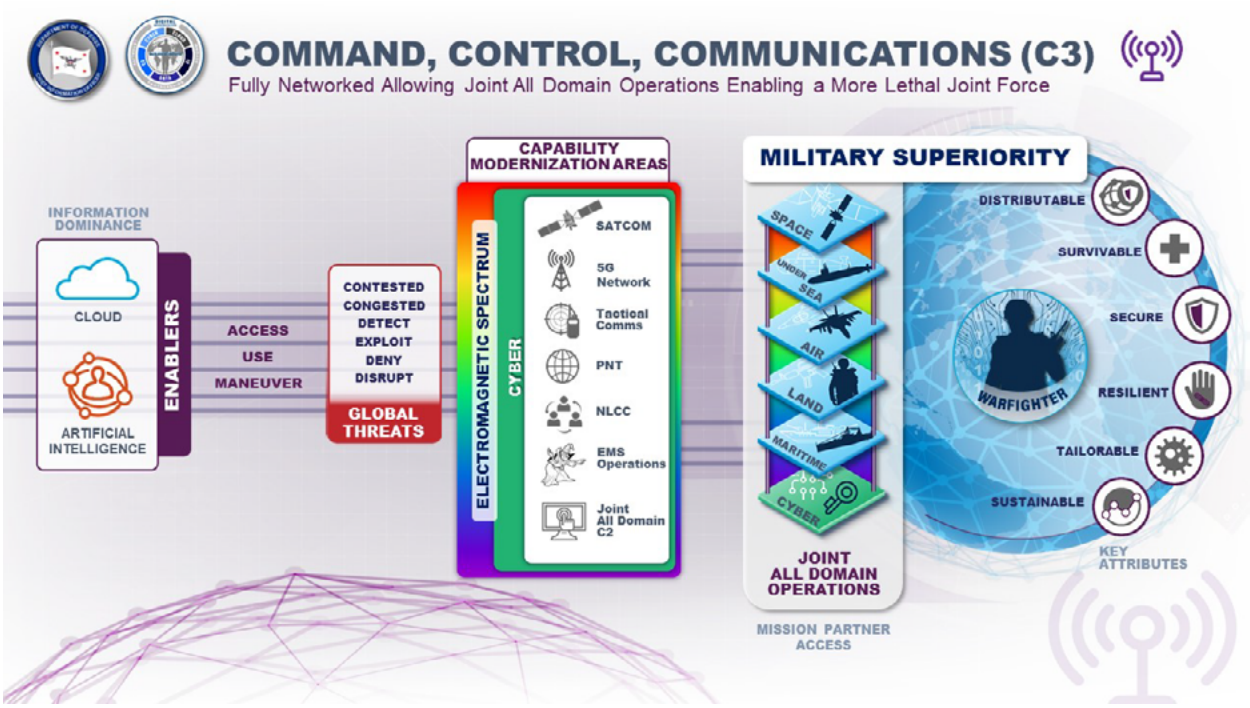

Figure 1: Command, Control, and Communications Modernization

This strategy focuses on C3 enabling capabilities that support effective joint and multinational operations (Figure 1). C3 enabling capabilities are composed of information integration and decision-support services, systems, processes, and related communications transport infrastructure that enable the exercise of authority and direction over assigned and attached forces. These capabilities enable commanders and decision makers rapidly to evaluate, select, and execute effective courses of action to accomplish the mission.

Specifically, this strategy provides the approach and implementation guidelines for modernizing C3 enabling capabilities in the 2020-2025 timeframe. As part of the *2018 National Defense Strategy* (NDS) implementation, the Joint Staff is developing joint and mission-partner networking concepts of employment for executing joint all-domain operations in contested environments. Informed by these concepts, the Office of the Under Secretary of Defense for Research and Engineering (OUSD(R&E)) is developing and evolving a long term (2024 and beyond) Fully Networked Command, Control, and Communications (FNC3) architecture. Implementing these future concepts and architectures will take time to mature new technologies and investment over many years. This C3 Modernization Strategy provides direction for bridging the gap between today's legacy C3 enabling capabilities and the future FNC3 enabled JADC2 to ensure the Joint Force is able to "fight tonight" while creating a viable transition path to the future technologies required for joint all-domain operations.

Strategic Environment

The NDS calls for a Joint Force that is more lethal, adaptive, and resilient; a Joint Force that can win on the battlefield by fighting into and within contested environments and gaining dominance in and across all domains. The NDS makes it clear that DoD cannot expect success in future military operations with yesterday's weapons or equipment. This is especially true of C3 enabling capabilities.

> *Adversaries studied the American way of war and began investing in capabilities that targeted our strengths and sought to exploit perceived weaknesses…. Such capabilities contest what was until recently U.S. dominance across the land, air, maritime, space, and cyberspace domains.*
>
> National Security Strategy, 2017

Since the end of Desert Storm, China and Russia have invested in capability and capacity to contest the United States' C3 superiority and freedom of access to, and maneuver in, the electromagnetic spectrum. Meanwhile, DoD's focus for the past 30 years has been on operations in permissive environments, prioritizing major investments for net-centric systems and cyberspace, vice advanced C3 capabilities required to operate successfully in highly congested and contested electromagnetic environments. The Department of Defense focused on a rapid Military Department-centric capability development and acquisition approach which decreased joint collaboration and increased the risk of duplication of effort at a time when the Joint Force needed to deepen interoperability and increase innovation to reduce costs.

New technologies such as fifth generation (5G) mobile networks, cloud computing, artificial intelligence (AI), and cognitive spectrum agility will accelerate the pace of change, reshaping how future military forces operate. To maintain strategic advantage, DoD must continuously modernize to keep pace with today's and future threats. Innovation through careful design and implementation of networked, enterprise C3 solutions capable of rapidly integrating new technology will deliver timely, data-driven decisions to the Joint Force.

Modernized C3 enabling capabilities will facilitate a secure, unconstrained flow of information from the source through cloud-enabled collection and processing nodes to delivery

anywhere in the battlespace at the right time. Hardened, survivable, and resilient C3 networks are critical to realizing the promises of cloud computing, AI, and other advanced capabilities for those who need them most – the Department's Soldiers, Sailors, Marines, Airmen, and Space Force personnel at the tactical edge.

The Joint Force, allies, and mission partners must have nimble access, use, and maneuver within the transport layer which is predominantly a radio frequency transmission path at the tactical edge. A fully networked Joint Force relies on a common C3 infrastructure from the application layer to the physical layer. This includes a shared data layer and common data standards that connect platforms and operators across every domain, regardless of Military Department or equipment vendor. This capability does not exist today. Current C3 architecture consists of multiple data formats, non-interoperable system interfaces, serial and stove-piped data flows that limit data discovery and analytics, and incompatible data-links requiring complicated relays to communicate between platforms, mission types, and operational domains.

These global challenges coupled with exponentially increasing warfighter demands for real time data drive the need to innovate and modernize C3 systems to provide warfighters a decisive information advantage. Effective joint all-domain operations are as much about information superiority as delivering overwhelming lethal force. The Department will preserve its military superiority against 21st Century peer competitors through its ability to gain and sustain near real time battlespace awareness, accelerate informed decision making via data analytics and AI, and enabling sensor-to-targeting information exchange in any domain to generate lethal or non-lethal effects. Future military operations will be powered by modern, networked C3 systems—distributable, survivable, secure, resilient, tailorable, and sustainable systems enabling a more lethal force.

Strategic Goals

This strategy presents C3 modernization goals aligned with and responding to the *DoD Digital Modernization Strategy* (DMS) and other higher level guidance including the NDS, *Department of Defense Cyber Strategy 2018*, *Capstone Concept for Joint Operations: Joint Force 2030*, and the Defense Planning Guidance. It implements near-term modernization actions and innovative solutions to provide competitive advantage through a more secure, effective, and efficient C3 environment. To this end, DoD must address these C3 modernization goals:

1. Develop and Implement Agile Electromagnetic Spectrum Operations;
2. Enhance the Delivery, Diversity, and Resilience of Position, Navigation, and Timing Information;
3. Strengthen National Leadership Command Capability;
4. Provide Integrated and Interoperable Beyond-Line-of-Sight Communications Capabilities;
5. Accelerate and Synchronize the Fielding of Modernized Tactical Communications Systems;
6. Fully establish and Implement a DoD Public Safety Communications Ecosystem;

7. Create an Environment to Rapidly Develop 5G Infrastructure and Leverage non-U.S. 5G Networks;
8. Provide resilient and responsive C2 Systems; and
9. Deliver Mission Partner Environment Capability and Services.

Figures 2 and 3 respectively, show the elements of the DMS implemented in this strategy and the alignment of goals and objectives between the two strategies.

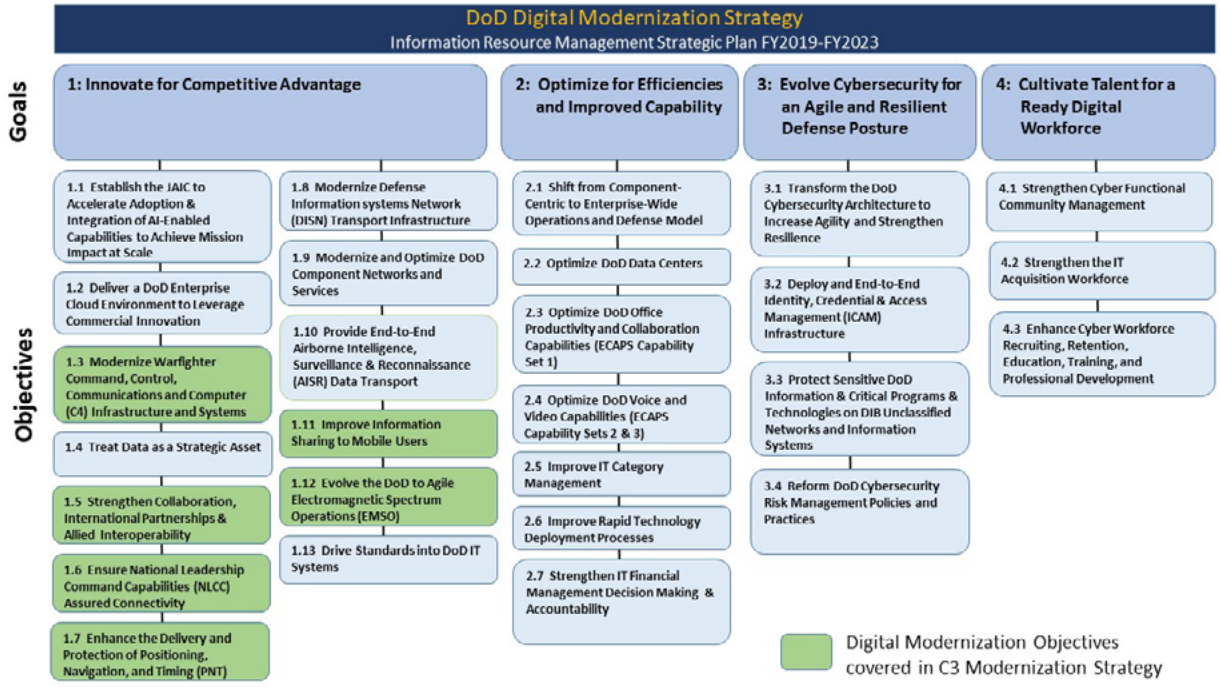

Figure 2: DoD Digital Modernization Strategy

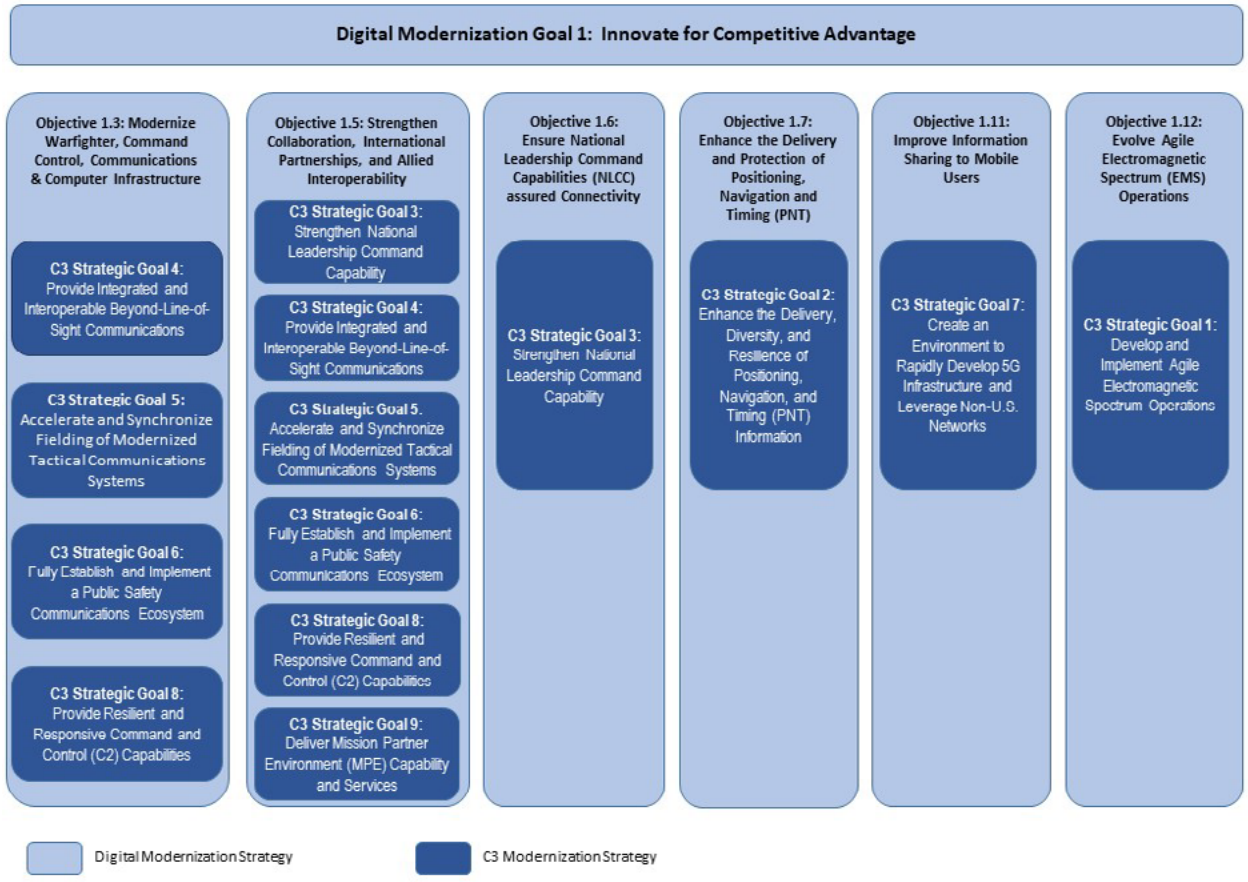

Figure 3: DoD C3 Modernization and Digital Modernization Strategy Alignment

DoD C3 relies on a complex, constantly evolving system of systems ranging from enterprise network infrastructure and core services to handheld radios and mobility devices at the tactical edge. The nine goals contained in this strategy are a finer-grain decomposition of the six DMS objectives highlighted in Figure 2. Other critical elements of C3 modernization including Joint Information Environment capability objectives, data centricity, and data analytics are included in the DMS, *DoD Cloud Strategy*, and the *DoD Artificial Intelligence Strategy*, respectively. Effective DoD enterprise governance will ensure successful synchronization and implementation of these strategies.

Goal 1: Develop and Implement Agile Electromagnetic Spectrum Operations

Electromagnetic Spectrum (EMS) superiority is a joint all-domain warfighting imperative. DoD operations and joint functions are increasingly dependent on Electromagnetic Spectrum Operations (EMSO). EMSO refers to coordinated military actions to exploit, attack, protect, and manage the electromagnetic environment. The Joint Force must have assured access, freedom of maneuver, and the ability to project power globally through all-domain operations. The EMS transcends all warfighting domains and enables mission execution within each. DoD will implement agile EMSO to support EMS superiority and enable JADC2.

Friendly forces face significant challenges operating in today's complex electromagnetic operational environment (EMOE). Congested conditions occur when adversary, neutral, and friendly actors concurrently participate in the EMS temporally, spatially, and spectrally to transmit, receive, and protect against effects of electromagnetic energy. Adversaries create contested conditions when they seek to impact friendly force operations by affecting friendly forces' ability to participate in the EMS. The laws of physics, national and international policy and regulations, and disruptive technologies create constrained conditions. Operations in a congested and constrained EMOE affect the ability of DoD to train as it fights, conduct tests of new weapon systems, and accomplish homeland defense operations. Mission accomplishment is disrupted when DoD's spectrum access is contested by adversaries fielding electronic attack and cyber technologies on the battlefield. Recognizing the increasingly congested, contested and constrained nature of the EMOE, DoD must maximize EMS access and freedom of maneuver and provide spectrum access when and where needed by the warfighter, while denying adversaries the same.

Today, C2 of EMSO is primarily executed through time- and resource-intensive processes using disparate automated and manual tools. DoD will modernize EMSO from a static-based approach to operationally-oriented activities that are agile, automated, and resilient. This modernization enables EMS superiority against peer competitors contesting the EMOE, allows DoD systems to access and use spectrum in congested environments without causing or incurring unacceptable interference, and supports the DMS objectives.

The EMS modernization effort shown in Figure 4 will be enabled by cloud-based and artificial intelligence technologies to deliver capabilities and services enabling dynamic EMS access and maneuver. EMS modernization will deliver greater lethality, effectiveness, and survivability of spectrum-dependent systems (SDS) across all domains. This implementation of agile EMSO enhances the resiliency and effectiveness of the increasing number of DoD SDS operating in congested, contested, and constrained electromagnetic environments. Agile EMSO will leverage modernized, networked C3 systems and support EMS superiority, which in turn enables joint all-domain operations.

The NDS three-pronged approach to enhance the effectiveness of our military against a broad range of potential threats provides the foundation to refine DoD's approach to compete and win tactical, operational, and strategic advantage across the EMS. Working with U.S. spectrum regulators, DoD will improve its ability to assess, contribute to, and adjust to worldwide regulatory and policy changes being proposed (e.g., repurposing spectrum to accommodate wireless services). DoD will utilize modern end-to-end spectrum capabilities to make spectrum access processes more responsive to DoD test, training, and operational needs.

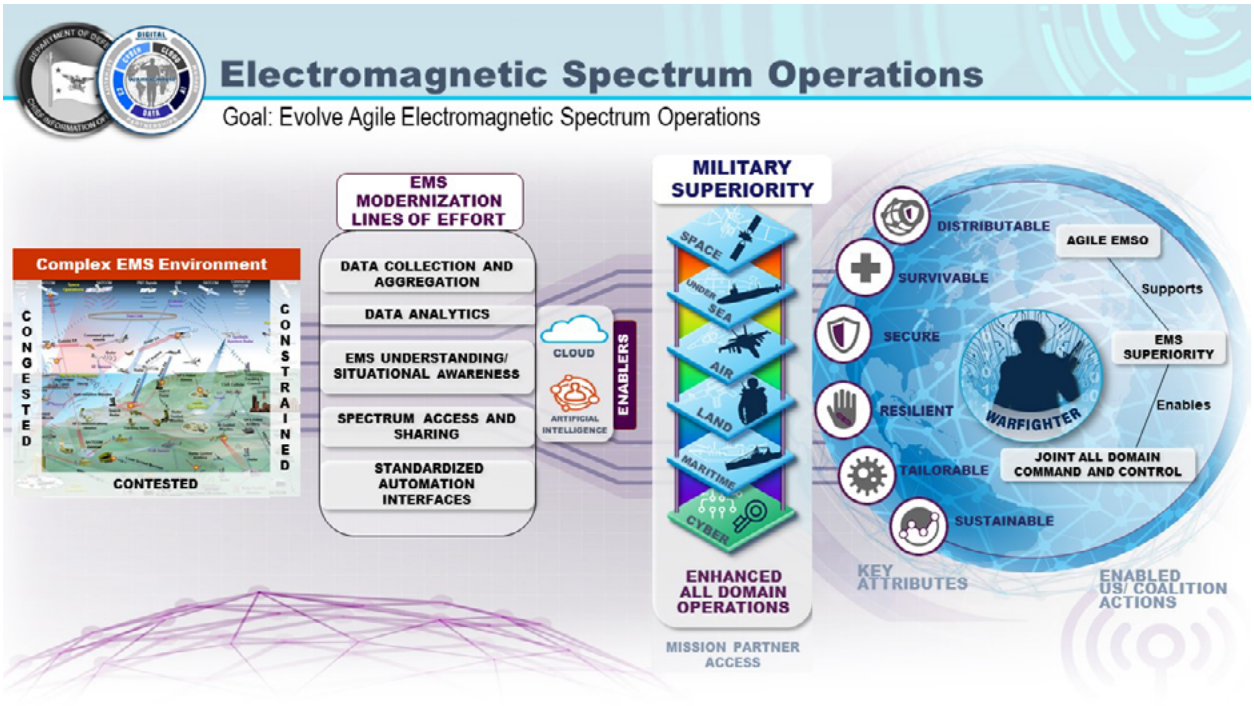

Figure 4: Electromagnetic Spectrum Operations

The Department is pursuing five lines of effort (LOE) to improve lethality through agile EMSO:

- **LOE 1.1 – Enhance EMS data collection and aggregation to provide accurate, relevant, discoverable, understandable, and trusted information.** In the near-term, DoD will enhance EMS data collection, provide modernized EMS data collection web services, and develop comprehensive cloud-based EMS databases that fuse data from multiple data sources. These capabilities are essential to the objective of performing EMSO in near real-time.
- **LOE 1.2 – Develop AI-enabled data analytics to enhance decision-making and capabilities for EMSO.** DoD will develop statistical data analytics in the near-term as a first step toward developing an AI-enabled spectrum decision engine that will dramatically improve DoD's ability to perform near real-time EMSO.
- **LOE 1.3 – Improve EMS understanding and situational awareness capabilities to characterize and mitigate the risks from congested and contested EMOE.** In the near-term, DoD will enhance visualization to support decision-making and monitoring capabilities.
- **LOE 1.4 – Develop cognitive, dynamic, spectrum access and sharing capabilities to provide the warfighter reliable EMS access when and where needed.** Electromagnetic compatibility analysis application development will increase the ability of DoD systems to share spectrum and/or operate compatibly with systems in adjacent spectrum bands without affecting system effectiveness or compromising operational safety in the near-term. Cognitive, dynamic spectrum management, informed by robust situational awareness, will enable greater spectral efficiency, and provide for the ability to prioritize

and ensure access depending on the criticality of the task being performed by the spectrally dependent system. This is enabled by the development and fielding of multi-function electromagnetic systems that can near-simultaneously perform sensing modes such as radar, communications, PNT and other modes.

- **LOE 1.5 – Implement standardized automation interfaces to allow spectrum dependent systems to accept, avoid, reduce, or transfer spectrum access risks dynamically as they occur.** In the near-term, the DoD Chief Information Officer (CIO) will publish the Electromagnetic Spectrum Enterprise Architecture (EMSEA) v1 as the reference architecture (RA) for command and control of joint EMSO. In the future, DoD will develop data and analytics standards, and spectrum security standards to manage EMS access risks. These standards will ensure spectrum availability risks are identified and managed at the early stages of spectrum dependent system requirements, planning, programming, and development. The EMSEA will also be updated on an annual basis to inform, guide, and constrain the transformation of EMSO as the modernization strategies are implemented.

Goal 2: Enhance the Delivery, Diversity, and Resilience of Position, Navigation, and Timing (PNT) Information

PNT information is inextricable from and vital to modern military operations, providing warfighters and weapons systems precise spatial orientation and time synchronization. Elements of PNT are embedded in and essential to the effective employment of virtually all DoD systems. These include: aviation navigation, maritime guidance and control, precision guidance munitions, and communications networks. DoD continues to lead the world in development and employment of PNT capabilities, building upon the strengths of the Global Positioning System (GPS), combined with other sources of accurate PNT information to increase resilience and accuracy.

To advance and support U.S. national security now and into the future, DoD must remain attuned to the vital enabling role that military PNT capabilities play in shaping the global environment, deterring aggression, fighting and winning today's wars, and preparing for future challenges.

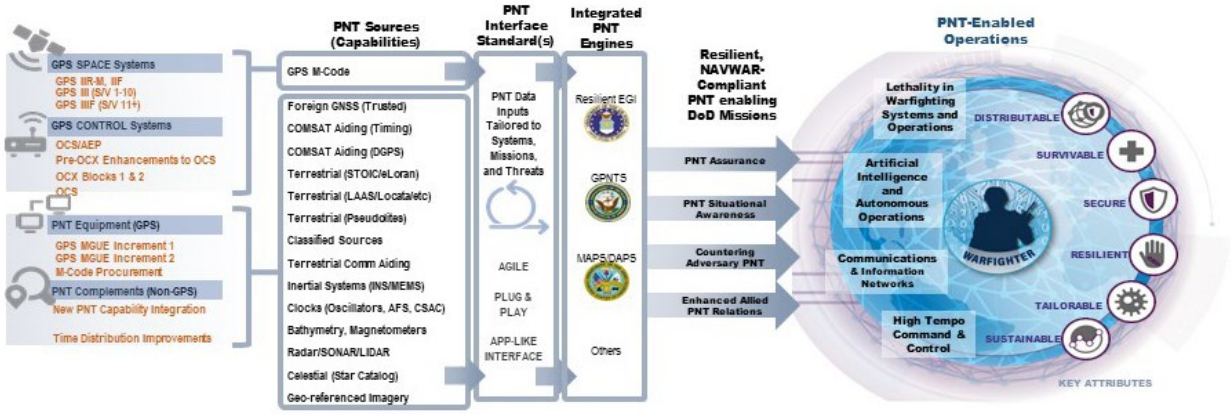

Figure 5: DoD PNT Enterprise

DoD will enhance the delivery, diversity, and resilience of PNT through the following lines of effort:

- **LOE 2.1 – Implement a modular open-system approach to integration of DoD PNT Enterprise capabilities to enable maximum flexibility and unpredictability in responding to the evolving navigation warfare (NAVWAR) threat environment.** A multi-source PNT open architecture will enable and promote agility and affordability while allowing each Military Department to "tailor" PNT capability combinations to achieve NAVWAR compliance in applications appropriate to each platform and mission in accordance with DoD Instruction (DoDI) 4650.08, *Positioning, Navigation, and Timing (PNT) and Navigation Warfare (NAVWAR)*. The key to achieving a fully usable and flexible open-system approach to PNT capability integration rests in agreement among the Military Departments on a set of input/output PNT standards to interface with platform data busses and enable multi-source PNT-enabled mission operations as well as platform operations, where necessary.
- **LOE 2.2 – Field modernized PNT capabilities.** GPS remains a cornerstone DoD PNT capability, and must continue to be modernized to meet warfighter needs. An initiative is now underway to strengthen GPS resiliency through expedited fielding of Military GPS User Equipment (MGUE), which incorporates the modern GPS Military Code (M-Code). Fielding plans for all planned MGUE recipients are consolidated in a master database managed and updated by DoD CIO. MGUE Increment 1 cards will be installed, as they become available, in high-priority DoD systems, supported by bulk-buy application-specific integrated circuits (ASICs). Lower size, weight, and power (SWaP) form factor Increment 2 cards will follow to meet special size and power applications.

  However, GPS vulnerability to threats from jammers and spoofers has long been acknowledged and must be addressed as GPS modernization proceeds. Consequently, to combat man-made and natural threats to GPS, other sources of PNT information will be necessary to assure continuous PNT service for military users. This will be accomplished through leveraging parallel DoD science and technology efforts to implement multi-source PNT capabilities in DoD systems using PNT modular open-system approaches. One key initiative in this area is the Air Force Research Laboratory's Navigation Technology Satellite 3 (NTS-3) program which is demonstrating a flexible payload that will inform future GPS augmentation options. NTS-3 and similar efforts will help ensure the Joint Force is equipped with PNT capabilities based upon system requirements and operational mission profiles that enable compliance for survivability in expected NAVWAR environments.
- **LOE 2.3 – Develop NAVWAR partnerships with allies and coalition partners.** DoD policy states that U.S. and allied forces must effectively employ NAVWAR to ensure a PNT advantage in support of military operations. This requires all DoD systems using or providing PNT information to become NAVWAR compliant (in accordance with DoDI 4650.08) and that compliance be tested and verified by appropriate DoD acquisition and test authorities. DoD is currently and will continue to conduct discussions and establish agreements with U.S. allies and coalition partners regarding acquisition and employment of PNT Enterprise capabilities to minimize collateral damage and ensure interoperability in combined NAVWAR operational environments.

- **LOE 2.4 – Cooperate closely with other federal departments and agencies regarding civilian use and modernization of GPS for peaceful purposes and facilitating access to appropriate levels of GPS services to meet requirements for homeland security purposes.** In executing these responsibilities, DoD will ensure the civil departments and agencies are aware of and are sensitive to the dual-use implications inherent in GPS and other PNT Enterprise applications. Many of the openly available PNT capabilities employed by civil departments and agencies and the public can pose a threat when used improperly or in unauthorized ways by hostile parties. Therefore, caution must be exercised by all parties in advertising and employing such PNT capabilities, whether for domestic purposes or internationally.

  DoD has a statutory responsibility, along with the Departments of Transportation and Homeland Security, defined in Title 10, U.S. Code, Section 2281, to write and publish a biennial Federal Radionavigation Plan (FRP) to reflect the policy and planning for Federally provided common use (i.e., systems used by both civil and military sectors) PNT radionavigation systems.

  DoD will continue to cooperate closely with the other Federal departments and agencies in preparation and production of the FRP with regard to the operation and modernization of the GPS and will support civil-funded modifications to the GPS to meet emerging civil requirements. DoD will continue to support Federal department and agency requests for access to military GPS capabilities as necessary.

Success along these lines of effort will provide and assure a PNT enterprise with services and capabilities available to the Joint Force, allies, and mission partners across the full range of military and national security operations.

Goal 3: Strengthen National Leadership Command Capability

The National Leadership Command Capability (NLCC) encompasses three broad mission areas: Presidential and senior leader communications; continuity of operations and continuity of government communications; and Nuclear Command, Control, and Communications (NC3).

In general, NLCC is defined as a construct encompassing DoD command, control, communications, computer, intelligence, surveillance, and reconnaissance systems and services that provide national leadership (regardless of location and environment) with diverse, accurate, integrated, timely, and assured access to data, information, intelligence, communications, services, situational awareness, warnings, and indications from which planning, understanding, and decision-making activities can be initiated, executed, and monitored.

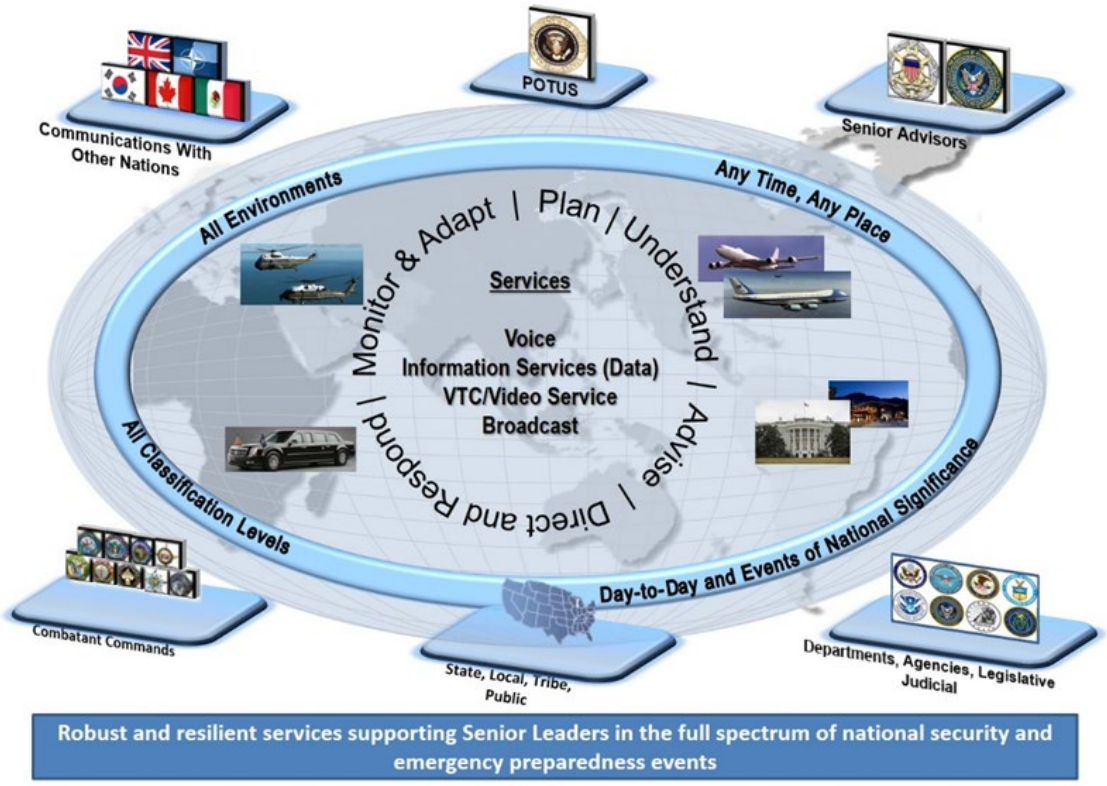

Figure 6: National Leadership Command Capability

NLCC communications systems and supporting resources provide the means for the President of the United States and other designated senior leaders to access the necessary information, decision support processes, and execution systems necessary to respond to any crisis, from any location, in any environment and/or during any threat condition. The NLCC is in place at all times supporting non/pre-event, event, and post-event periods.

Senior Leader and Continuity Communications

DoD will protect current senior leader and continuity communications capabilities while at the same time rapidly developing, integrating, and fielding new capabilities through the following four lines of effort:

- **LOE 3.1 – Sustain secure senior leadership and continuity communications.** Ensure that the capabilities required to conduct operations under all-threats and in all-hazards scenarios are available.
- **LOE 3.2 – Modernize senior leadership and continuity communications that are secure, resilient, and reliable.** Consistently evaluate and provide solutions appropriately scaled with requisite core enterprise services.
- **LOE 3.3 – Ensure the cybersecurity of senior leadership and continuity communications.** Include dedicated cybersecurity sensors and monitoring equipment to detect cyber-attack or intrusion that mitigate operational risk before systems are degraded or compromised.

- **LOE 3.4 – Ensure DoD C3 systems are interoperable with and capable of information sharing between NLCC and the broader National Security and Emergency Preparedness capabilities including interagency, State, local, tribal and territorial governments.** Current public safety Information technology and procedures are comprised of complex, disparate combinations of systems and capabilities. These support call taking, response alert, dispatch, and ongoing operational communications. DoD systems enterprise-wide should be modernized and interoperable with capability gaps mitigated between NLCC, DoD Public Safety Communications (PSC) and Civil PSC enterprises.

Nuclear Command, Control, and Communications

The third NLCC mission area is NC3. The system provides the functional C3 capability for nuclear deterrence and operations through a survivable network of communications and warning systems that ensure dedicated connectivity from the President to nuclear-capable forces. It must provide control of U.S. nuclear forces at all times, even under the enormous stress of a nuclear attack, assure the integrity of transmitted information, and possess the resiliency and survivability necessary to reliably overcome the effects of a nuclear attack. During peacetime and crisis, the NC3 system performs five crucial functions: detection, warning, and attack characterization; adaptive nuclear planning; decision-making conferencing; receiving Presidential orders; and enabling the management and direction of forces.

U.S. NC3 must be increasingly flexible to tailor deterrence strategies across a range of potential adversaries and threats, and enable adjustments over time. This ensures the DoD will maintain the range of flexible nuclear capabilities needed to ensure that nuclear or non-nuclear aggression against the U.S., allies, and partners will fail to achieve its objectives and carry with it the credible risk of intolerable consequences for potential adversaries now and in the future. These characteristics underscore the need for assured, reliable, and resilient communications across the full spectrum of conflict.

Today's NC3 system is a legacy of the Cold War, last comprehensively updated almost three decades ago. It is now subject to challenges from both aging system components and new, growing 21st Century threats. Of particular concern are expanding threats in space and cyber space, adversary strategies of limited nuclear escalation, and the broad diffusion within DoD of authority and responsibility for governance of the NC3 system, a function which, by its nature, must be integrated.

In light of the critical need to ensure our NC3 system remains survivable and effective, the DoD will pursue a series of initiatives. These include: strengthening protection against cyber threats, strengthening protection against space-based threats, enhancing integrated tactical warning and attack assessment, improving command post and communication links, advancing decision support technology, integrating planning and operations, and reforming governance of the overall NC3 system. These initiatives and associated actions are being implemented separately from this strategy as part of the nuclear enterprise modernization.

Goal 4: Provide Integrated and Interoperable Beyond-Line-of-Sight (BLOS) Communications Capabilities

Satellite Communication (SATCOM) is the primary means of BLOS communications for military operations, providing an unparalleled capability to distribute high-volume data globally. However, despite sustained efforts to launch new satellite constellations and continuing use of contracted commercial satellite bandwidth, today's BLOS capabilities are inadequate for future operations in denied-disconnected, intermittent, and low bandwidth (D-DIL) environments for the following reasons:

- Demand for bandwidth continues to increase beyond the Department's ability to bring new satellite assets into operation and to obtain commercial contracted bandwidth. This is particularly acute in areas where there is little civilian demand for service (e.g., open ocean, high latitudes, and areas with sparse or severely impoverished populations).
- A large percentage of existing satellite bandwidth is susceptible to electronic warfare and cyber-attack, adding substantial risk to operations in contested environments.

The Department must respond to this situation through a multi-pronged approach of modernizing the DoD SATCOM enterprise, enhancing existing technology including high frequency (HF) communications, and pursuing new BLOS technologies:

- **LOE 4.1 – Establish and continuously monitor strategy, policies, procedures, and other elements of the DoD SATCOM governance framework.** The DoD CIO, U.S. Space Force (USSF), and the Space Development Agency in close coordination with United States Space Command (USSPACECOM) and U.S. Cyber Command (USCYBERCOM) will deliver SATCOM governance in support of tightly integrated, hybrid military and commercial, Enterprise SATCOM Architecture. The DoD CIO will enforce governance decisions through the Capability Planning Guidance (CPG) and oversight of Military Department budgets to ensure compliance with SATCOM-related modernization initiatives.
- **LOE 4.2 – Conduct requirements-informed architecture planning activities to establish a responsive, resilient, integrated DoD SATCOM enterprise.** The DoD CIO, in coordination with the Space Development Agency and industry, will develop top-level Reference Architectures (RAs) to guide USSF solution architectures in the delivery of seamless SATCOM capability for the warfighter. RAs will satisfy warfighter requirements and provide the necessary guidance to drive resiliency, flexibility, and interoperability in fielded solutions. Developed architectures will form the basis for future analyses of alternatives (AoA) and provide the necessary warfighter reach-back for cloud, artificial intelligence (AI) and cyber capabilities.
- **LOE 4.3 – Expand SATCOM cooperation and integration with Allies and International Partners.** The DoD CIO and the Department of the Air Force's International Affairs (SAF/IA) team continue to expand access to and participation with international partners in U.S. Military SATCOM capabilities and also seek opportunities for the United States to participate in and have access to International Partner SATCOM capabilities. The DoD CIO and USSF must continue to lead and remain engaged in international forums and Allied organizations such as the North Atlantic Treaty Organization (NATO).

- **LOE 4.4 – Acquire and field modernized DoD SATCOM capabilities for delivery of information services to the tactical edge.** The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) in close coordination with OUSD(R&E) and the USSF will provide capability portfolio management to acquire, align, and field SATCOM capabilities to meet joint warfighter needs. Additionally, the DoD CIO will ensure Defense Information Systems Agency (DISA) and the Military Departments acquire and field synchronized SATCOM gateway and user terminals as part of the overall integrated and hybrid SATCOM architecture. The DoD CIO will ensure SATCOM capabilities are compliant with SATCOM RAs to ensure interoperability, flexibility, and resiliency and the ability to execute Enterprise Management and Control (EM&C).
- **LOE 4.5 – Conduct Informed and responsive DoD SATCOM resource management.** The DoD CIO through its SATCOM Enterprise Management and Control Reference Architecture (EM&C RA) and the USSF's fielded EM&C solutions will deliver integrated and seamless management of SATCOM resource allocation and provisioning. EM&C capabilities require the USSF to have comprehensive situational awareness to overcome and operate through electromagnetic interference (EMI) and the ability to move users across commercial and military purpose-built SATCOM systems.
- **LOE 4.6 – Develop and deliver advanced BLOS capabilities for SATCOM-denied environments.** Once a mainstay of BLOS communications, the use of HF communications diminished with the proliferation of SATCOM. However, the current threat environment coupled with advances in HF internet protocol-enabled software defined radios, digital beamforming antennas, digital signal processing, networking, multi-function systems, and wideband technologies make HF a necessary and effective alternative to SATCOM in D-DIL environments. The DoD must modernize its HF enterprise, both the HF Global Communications System (HFGCS) and the strategic and tactical platforms, with these technologies. The DoD must also pursue other innovations such as relay, range extension, and cross-banding capabilities to bridge the communications gap in SATCOM denied environments.

These modernization activities support and enable warfighter access to cloud, AI, and cyber operations capabilities in locations around the globe where DoD Information Network (DoDIN) infrastructure is denied, degraded, or non-existent. The goals of the National Security Strategy and National Defense Strategy are supported and advanced by this Department focus on DoD BLOS communications capabilities and the crucial role they play in fighting and winning today's wars and in preparing for future challenges.

Goal 5: Accelerate and Synchronize Fielding of Modernized Tactical Communications Systems

Today's tactical communications landscape is complex and fragmented. It is comprised of many diverse systems fielded by independent program offices, driven by Military Department-centric requirements that did not prioritize enterprise level performance, interoperability, and security of tactical networks. The result is a battlefield mixture of legacy and digital capabilities consisting of more than one million terminals fielded across thousands of Military Department, ally, and coalition partner platforms connected by hundreds of distinct waveforms and systems with numerous sub-variants. Disjointed fielding of non-interoperable tactical waveforms drove the

need for gateways, further complicating the architecture and reducing the resiliency of the most operationally relevant communications systems. Rapid advances in communications information technologies and the changing character of modern warfare require a smarter, synchronized approach to fielding tactical communications that deliver the Joint Force a decisive information advantage over our adversaries.

The Department must synchronize efforts to deliver a tactical communications network comprised of intuitive, standards-based capabilities adapted to commanders' requirements for information sharing, collaboration, and interoperability across all domains. To achieve this, DoD will implement the following lines of effort:

- **LOE 5.1 – Mature tactical communications enterprise governance to guide fielding decisions and synchronize Military Department efforts.** The Department must change its focus from stove piped, platform centric C3 systems to a fully-networked enterprise approach. Ongoing Military Department modernization efforts provide incremental tactical C3 improvements but DoD lacks the unity of effort and cross-Service synchronization necessary to field survivable, effective, and suitable capabilities to conduct all-domain operations of the future. The Department will utilize a Command, Control, and Communications Leadership Board (C3LB), a Tactical Communications Senior Steering Group (TCSSG), the Joint All-Domain Command and Control Cross Functional Team (JADC2 CFT), and other appropriate governance bodies to provide strategic direction, prioritization, policy execution, and resourcing recommendations for successful C3 capability modernization. The TCSSG will focus on sustainment and modernization of existing waveforms, and acquisition of future waveforms in the context of modernization roadmaps developed in conjunction with Military Departments and OUSD(R&E).
- **LOE 5.2 – Develop and enforce policies and standards to improve interoperability and reduce tactical grid complexity while enhancing resilience.** Smart policy and transparent processes underpin effective governance. The Department will develop new or revise existing policy to prescribe procedures for oversight and management of DoD tactical C3 enterprise capabilities. These policies will specify enforceable processes for guiding development, synchronizing modernization investments, and the integration of tactical C3 capabilities necessary for the employment of a more lethal Joint Force. Additionally, tactical communications enterprise governance bodies will ensure standards and specifications for DoD waveforms include performance criteria, standardized data and equipment interfaces, and interoperability specifications.
- **LOE 5.3 – Develop and publish approved joint tactical communications architectures and modernization roadmaps to enhance secure, real time/near real time tactical communications with joint, allied, coalition, and partner forces.** To achieve success in joint all-domain operations, the Department needs a common set of RAs and joint roadmaps to deliver a robust tactical network capable of executing all-domain concepts of employment. Today, the Combined Joint Task Force (CJTF) Architecture Model provides a tool for modeling and analyzing projected Joint Force communications transport capabilities in an operational environment. However, the CJTF Architecture Model is not an approved enterprise architecture and therefore not recognized as an authoritative document for measuring interoperability and influencing Military Department's tactical C3 investments. The DoD CIO, in coordination with the Joint

Staff, Military Departments, and other stakeholders will develop a new CJTF RA that defines the interfaces between the various elements of the tactical network to enhance interoperability and information exchange across warfighting domains.

Once completed, the CJTF RA will serve as the blueprint for a Joint Tactical C3 Modernization Roadmap that will provide an integrated plan for tactical C3 modernization and technology deployment. The roadmap will include target timelines for implementing interoperability and performance enhancements to deliver resilient solutions for contested environments and will serve as a tool for assessing Military Department modernization investment strategies.

- **LOE 5.4 – Sustain and modernize tactical communications network capabilities by rapidly integrating modern communications technologies to improve the capability and survivability of DoD tactical networks.** The existing tactical communications landscape is too diverse, fragmented, and complex to incorporate all legacy devices and systems into a future fully-networked C3 architecture. The Department must focus modernization efforts on waveforms and systems that possess or can be enhanced for increased survivability, effectiveness, and suitability in contested environments as well as more benign environments. Informed by Joint Staff developed future concepts of employment and under the guidance of the C3LB, the Department must identify key sections of the Joint Tactical Grid (JTG) where modernization must be prioritized. JTG is the warfighting networks component of the JADC2 architecture that enables Joint and coalition warfighting concepts and exchanges critical warfighting data. Other waveforms and networks that do not support the JTG and draw resources away critical Department waveforms must be identified and retired. Gaps in capability in the JTG must be identified and filled with enhanced existing waveforms or future waveforms. These analyses will drive updates to the C3 architecture, standards, and modernization roadmap, enabling the Military Departments to develop clear fielding priorities and timelines to inform investment decisions.

These efforts serve as a basis for a joint enterprise approach to tactical communications modernization, required for delivering joint warfighters a decisive, joint, all-domain information advantage throughout the full range of military operations from permissive environments to highly-contested great power engagements.

Goal 6: Fully Establish and Implement a Public Safety Communications (PSC) Ecosystem

One of the Department's greatest responsibilities is the safety and protection of the public. The PSC mission area encompasses all matters pertaining to communications systems relevant to public safety, emergency management, and mass notification activities. It requires the collective collaboration of publically available information in a unified messaging format leveraging DoD's permanent telecommunications infrastructure for routine and critical emergency information, via host State/territory/nation electronic connections, between each of the supporting and supported public safety mission partners' ecosystems.

Commanders and agency directors require reliable and available emergency response capabilities to conduct safety of life, safety of flight, and preservation of property response activities within each of the thousands of DoD installations, facilities, training areas, and assigned

areas of operations. DoD must integrate with national and international public safety mission partners to fulfill its PSC mission.

Starting in Fiscal Year 2019, DoD added PSC to the DoD CIO mission portfolio and initiated action to incorporate this mission area within DoD's Enterprise Architecture. DoD will align regulations and integrate its telecommunication infrastructure with national and international public safety communications systems. DoD CIO has established four lines of effort to fully establish and implement a PSC ecosystem across the entire doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy (DOTMLPF-P) framework:

- **LOE 6.1 – Develop DoD policy and apply governance.** Elevate PSC as a critical core capability within DoD to increase preparedness for emergency and disaster response. Develop policy to align all elements of DoD to gain efficiencies in cost and capability equal to and interoperable with State, local, tribal, and host nation public safety communications technology, procedures, and interaction. Governance will take the form of a chartered working group where stakeholders coordinate and align strategic initiatives to facilitate implementation of resilient and interoperable emergency response capabilities.
- **LOE 6.2 – Assess and mitigate capability gaps.** The current DoD public safety Information technology and procedures are comprised of complex, disparate combinations of systems and capabilities. These support call taking, response alert, dispatch and ongoing operational communications. DoD will conduct an enterprise-wide assessment to determine the baseline of tools, capabilities, and costs for PSC modernization. Implementation actions will be developed to mitigate capability gaps and modernize the DoD PSC enterprise across DoD installations.
- **LOE 6.3 – Synchronize DoD budgeting, Program Objective Memorandum (POM), and spending.** To modernize PSC across DoD in the most efficient manner, DoD components must realign future budgeting and spend plans. Use of common commercial or government off the shelf solutions and coordinating plans, budgets, and spend plans will be the basis for future budgeting. By establishing a PSC focused program element across the Future Years Defense Program (FYDP), DoD will begin to align funding decisions with coordinated priorities to maximize PSC capability and minimize duplication of effort and overall costs.
- **LOE 6.4 – Develop active partnerships and engage with industry.** DoD PSC professionals and executives will seek to establish State, local, tribal, host nation, and interagency partnerships though memorandum of agreements, professional collaboration, and industry interaction. Operators and managers will engage to remain current with PSC education, training, exercise, and certification. DoD PSC professionals will meet national and international requirements and standards to promote collective collaboration, unified messaging, and maintain mission essential capabilities.

Once the PSC mission area is established across the DOTMLPF-P framework, DoD will plan, resource, communicate, and coordinate its interest with each of the supporting public safety government authorities and telecommunication service providers to ensure reliable and available emergency response capabilities to conduct safety of life, safety of flight, and preservation of property response across DoD.

Goal 7: Create an Environment to Develop 5G Infrastructure Rapidly and Leverage Non-U.S. 5G Networks

The Department is actively supporting the National Security Council's established goal to improve America's digital infrastructure by deploying and experimenting with 5G at military facilities nationwide in response to the President's commitment to making America first in 5G wireless technology.

DoD activities are designed to create an environment that will permit the Nation's telecommunication industry to develop and implement 5G infrastructure rapidly. Current lines of effort, ranging from policy coordination to research in applying 5G network concepts, include:

- **LOE 7.1 – Identify additional spectrum for 5G.** Work with the Federal Communications Commission and National Telecommunications and Information Administration to assist in the identification of additional spectrum for 5G operations.
- **LOE 7.2 – Harmonize 5G spectrum across the globe.** Join forces with the State Department to identify and harmonize, wherever possible, 5G spectrum across the globe. Spectrum harmonization, the uniform allocation of radio frequency bands across a region, reduces radio interference along borders and helps in international roaming and interoperability.
- **LOE 7.3 – Develop 5G standards, spectrum, and cybersecurity policy.** OUSD(R&E), in coordination with appropriate Principal Staff Assistants and other Component heads, will lead the DoD effort.
- **LOE 7.4 – Accelerate DoD's adoption of 5G technology.** Provide at-scale test facilities that enable rapid 5G experimentation and dual-use application prototyping.

Ultimately, 5G will provide "more data quicker" and will transform both commercial and military mobile platform delivery services and applications including autonomous vehicles, bioinformatics, internet-of-things, and tactile internet. 5G has the potential to become the communication fabric that supports new efforts in cloud based AI enhanced distributed sensing. In this regard, DoD will be both an enabler and user of 5G, supporting the growth of the Nation's digital economy while advancing operational effectiveness.

Goal 8: Provide Resilient and Responsive Command and Control (C2) Capabilities

Leaders must have the ability to command, control, and coordinate an interdependent force in rapidly changing scenarios involving complex, distributed, simultaneous, or sequential operations. More than ever, the Joint/Combined Force will include long-standing and ad-hoc mission partners at the national, state, local, tribal, interagency, and international levels. To meet this need, the Department must design, develop, deploy, and operate accessible, survivable, and resilient integrated capabilities that provide leaders and their assigned forces visibility of and easy access to information at the speed of relevance. This allows everyone in the chain of command to quickly grasp a situation and effectively support a commander's intent, decision making cycle, and the elements of mission command. Authorized users must be able to see, understand, plan, decide, and act on secure, authoritative, and trusted information.

The overarching goal is to provide C2-enabling capabilities that connect distributed sensors, data, and effects from all domains to decision makers at the scale and tempo required to accomplish commander's intent—agnostic to domains, platforms, or functional lanes. Leader-centric, joint all-domain C2 is a transformational concept whereby a commander or senior leader can use any authorized device to: quickly gain situational awareness and understanding; communicate, coordinate, and collaborate with whoever needed; decide on a course of action based on trusted information at hand; and act to convey their intent in the exercise of mission command. Authorized users must be capable of independently acting on that intent and decisively execute operations while also communicating, coordinating, and collaborating with whomever they need, in a trusted and secure information environment. Mission partners must seamlessly integrate with joint forces with the capabilities to interoperate, communicate, coordinate, and collaborate as the mission dictates. Mobile devices must be capable of recognizing user identity credentials and allow seamless and appropriate access and management of information. Data must be visible, accessible, accurate, trusted, understandable, and interoperable, with information flowing seamlessly across security boundaries as required.

JADC2 reflects a comprehensive movement in DoD acknowledging the problems with globally-integrated operations and the inability to maintain decision/operational advantage while countering adversary strategies. This resulted in the assembly of a CFT, endorsed by the Secretary of Defense on January 31, 2020, to bring stakeholders together to solve the challenge of Joint C2. JADC2 evolved sporadically over the last decade, but gained momentum over the last three years as the focus shifted toward peer threats able to challenge U.S. dominance in all domains. The "2017 National Security Strategy" and "2018 National Defense Strategy" sharply focused the Department on long-term strategic competition and the pursuit of seamless integration. Concurrent advances in AI, cognitive aiding, and man-machine interface demonstrate not only the potential to expand integration along these lines, but also to improve speed and quality of decision making.

Uniformly, anti-access/area denial strategies drive a need to disperse forces and headquarters across more locations and over greater distances. This necessitates extended communication pathways, long range surveillance and effects, and an increased need for smaller units to operate independently, often in D-DIL environments. Fighting under these conditions, smaller distributed elements must be able to re-aggregate and reinforce one another. Multi-domain battlespace awareness becomes necessary to C2 the battle and converge Joint Force and mission partner capabilities across all domains, the electromagnetic spectrum, and the information environment. Integrated closely with allies and multinational partners, the level of interoperability, C2 flexibility, and multi-spectrum mesh connectivity needed between all sensors to all shooters requires a robust, protected, and resilient network that enables integrated fires even in a contested environment. Flexible integration of emerging technologies (AI, self-healing networks, etc.) and the ability to bridge multiple classification levels across agile organizational structures is essential to making this possible.

JADC2 strives to make these principles the new norm. Each Military Department has developed expanded-domain C2 concepts and solutions in recent years and their efforts are gradually converging. However, there is no unifying vision to ensure these related efforts are mutually supportive leading to mostly Component-unique solutions. C2 is ultimately a joint problem that no individual Military Department can solve. To understand Joint warfighter needs, the Department will first examine the impetus of individual Military Department efforts and

understand the common factors that drove them down similar and sometimes divergent paths. The Department must exploit these commonalities and synchronize the multiple efforts to a common, holistic architecture nominally depicted below.

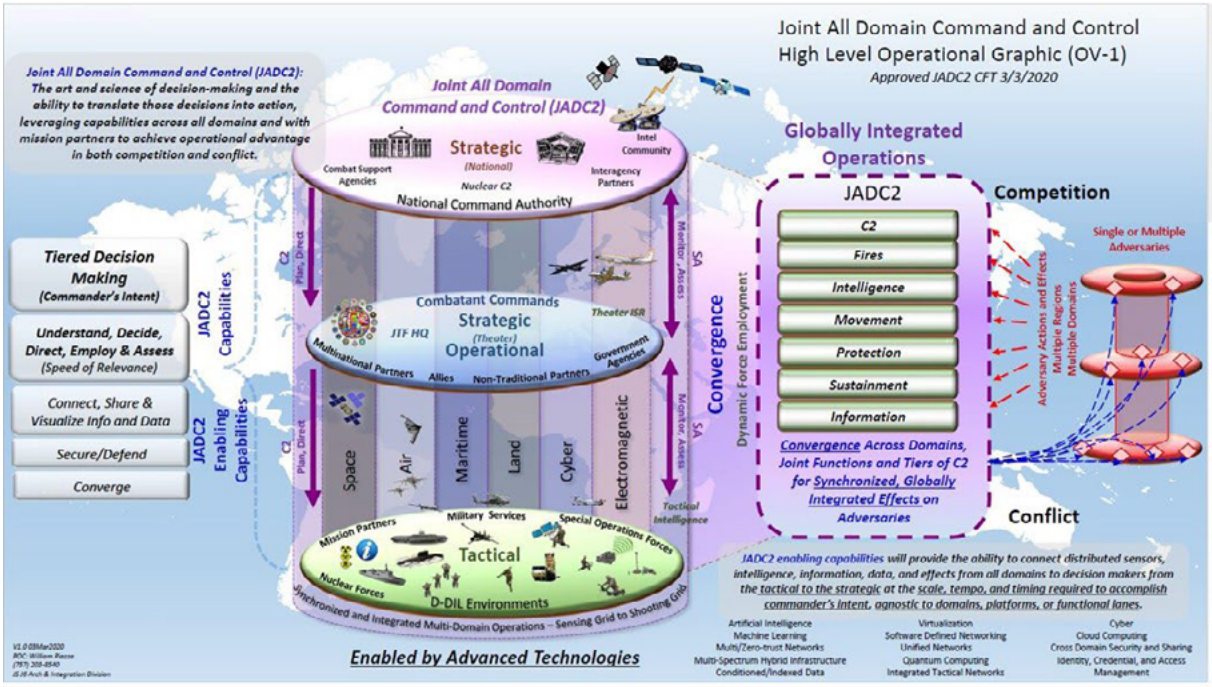

Figure 7: JADC2 Operational View

More than merely addressing targeting and kill chains, JADC2 must enable globally integrated operations with tools that support integrated all-domain warfighting. Commanders today lack capabilities to accelerate the processes to seamlessly converge effects at speed across all domains. Individual Military Department solutions are likely not sufficient for all. They require a higher-level concept and strategy to align efforts and ensure all solutions are complementary and reinforcing. A joint warfighting concept and modernized C2 concept are already in development and the JADC2 ideas should mature concurrently with any joint multi-domain operations-equivalent concept. To bridge these efforts, the Department is developing an overarching campaign plan under the direction of the JADC2 CFT that will collectively move the Military Departments in a common direction. The concept work must begin now to capture existing efforts and drive productive experimentation while continuing to expose the full complexity of the problem. The joint C2 system (people, process, technology) can provide a conceptual organizing structure to share and accumulate quick wins and would expedite DOTMLPF-P analysis of both near- and potential far-term solutions.

U.S. allies and mission partners are key players in the future joint all-domain fight and must be included where possible in the planning and development of JADC2 concepts and capabilities. They are conducting their own C3 planning and development activities and, as such, their experience may very well inform and benefit DoD efforts. The inclusion of key mission partners early in the process will promote and facilitate interoperability during the implementation phase and help mitigate delays and catch-up costs. Given the importance of the mission partners in the future fight, JADC2 concept and capability development must be integrated with development of

the Mission Partner Environment (MPE). This will ensure JADC2 information-sharing standards, processes, C2 systems, software, and cybersecurity are supported by and integrated with MPE standards and solutions.

The Department is pursuing four lines of effort to enable this goal:

- **LOE 8.1 – Implement Joint All-Domain C2.** Engage in concept development, joint experimentation, and demonstrations to rapidly evolve and implement the concept.
- **LOE 8.2 – Modernize command and control systems.** Transition to an accessible, resilient and survivable hybrid cloud based solution to provide all-domain joint situational awareness, and command and control, supporting enterprise, operational and tactical level capability with adequate training for superior operator proficiency and commander decision support.
- **LOE 8.3 – Implement information-sharing standards.** Expose legacy systems' authoritative data sources and develop new systems interfaces using a common interface standard in order to improve interoperability, operational agility, and set the conditions for improved machine-to-machine transactions.
- **LOE 8.4 – Promote software agility and increased cybersecurity.** Speed capability to the warfighter leveraging enterprise cloud solutions, Agile and Development Security Operations (DevSecOps) acquisition approaches, and cybersecurity advancements.

DoD Components must prioritize capabilities, improve fielding processes, and increase resources as necessary to modernize joint and component level C2 systems and services. Emphasis must be on improving joint all-domain situational awareness, modernizing joint planning and execution capabilities, enhancing capabilities for force employment to increase lethality, and improving resilience and readiness of deployable joint C2 capabilities. Modernization efforts will leverage technical advances in enterprise-based solutions for cloud, AI, and cybersecurity to achieve operational advantage in both competition and conflict by rapidly executing inside the enemy's decision cycle.

Goal 9: Deliver Mission Partner Environment (MPE) Capability and Services

In order to defend the Nation and enhance global interoperability DoD must promote effective information exchange among: other Federal, State, local, and tribal departments and agencies; allies, mission partners, host nations, and other nations; U.S. and international non-governmental organizations; multinational treaty organizations; and private sector organizations. Releasable DoD information should be visible, accessible, understandable, trustworthy, secure, interoperable, and made available to appropriate mission partners, to the maximum extent allowed by U.S. law or DoD policy. Any technology solution must be integrated with the development of JADC2 based on a common set of standards, protocols, and interfaces to enable the sharing of releasable DoD data, information, and information technology (IT) services. To the maximum extent possible, these common DoD information sharing standards, protocols, and interfaces will be compatible and interoperable with those of other federal departments, agencies, and mission partners. DoD will also use a comprehensive, widely understood MPE governance framework for creating and sustaining a federated information sharing community of organizations

and individuals. The MPE is the DoD solution to meet these requirements. This MPE framework shall:

- Enable coalition and Joint Force commander's access to an MPE that supports required training and conduct of operations with authorized mission partners at any time.
- Provide strategic, operational, and tactical flexibility for all commanders to execute C2 and intelligence actions by providing the means to communicate commander's intent clearly to achieve unified action.
- Leverage a federated network concept supporting the connection of multiple networks and national systems with applications and tools to enable mission partner information sharing for a given operation.

The Department is pursuing three lines of effort to enable this goal:

- **LOE 9.1 – Establish policy and procedures for a DoD-wide MPE framework.** Align policy, responsibilities, procedures, and resources for implementation of an MPE capability that responds to the full spectrum of conflict, humanitarian and disaster relief operations, defense support of civil authorities (DSCA), and U.S./Non-U.S. led cooperative security activities.
- **LOE 9.2 – Transition from disparate legacy solutions.** Updated capabilities will be fielded that are interoperable with a modernized and standardized MPE infrastructure.
- **LOE 9.3 – Application of interoperability compliance and assessment.** Mission-based interoperability compliance and assessment capabilities are required to provide a high level of confidence that information can be exchanged with whom it is required, when and where it is required, as determined by operational need and the accepted level of risk.

Implementation

The strategic goals and associated lines of effort in this strategy provide the overarching direction for modernizing C3 enabling capabilities and set the foundation for a fully-networked C3 infrastructure capable of executing joint all-domain operations against 21st Century threats. Successful execution requires operationalizing the strategy through detailed implementation plans and performance measures that identify and mitigate threats, ensure effective supply chain security, and incorporate secure engineering practices, to include initial and continuing test, evaluation, and remediation of weaknesses and vulnerabilities.

The implementation appendix provides high-level guidance to prioritize and synchronize modernization efforts aligned to the various goals contained in this strategy. DoD CIO will drive execution and track progress through established processes which include the DoD CIO CPG issued annually to inform Component Program Objective Memorandums; tracking key metrics through the DoD Annual Performance Plan and Annual Performance Report; and DoD CIO's annual review and certification of Component information technology related budget submissions.

Successful implementation of the strategy also requires strong stewardship through effective governance. The DoD CIO will establish an enterprise governance framework to foster

collaboration and create synergy among the many DoD stakeholders with statutory responsibilities in the C3 arena. Governance bodies will provide strategic direction, coordinate resource allocation, and align policy guidance to ensure cohesion of the Department's C3 modernization efforts.

Conclusion

DoD is facing an unprecedented era of change and opportunity in the C3 arena. Rapid advances of new government and commercial technologies offer promise for revolutionary improvements in military C3 capabilities. To realize and derive competitive advantage from these improvements, DoD must commit to decisive leadership, clear actions, and a joint enterprise approach to C3 modernization efforts.

In execution of this strategy, DoD directly responds to the NDS call to deliver our warfighters a decisive competitive advantage across the full range of military operations. Modernized C3 capabilities will enable *a more lethal force* through increased battlespace awareness, improved cross-domain maneuver and fires coordination, and more reliable and resilient communications among dispersed forces in complex environments. They will *strengthen alliances and deepen coalition interoperability* by allowing mission partners to integrate with Joint Forces seamlessly with the capabilities to interoperate, communicate, and collaborate as the mission dictates. Modernized C3 systems will support *Department reform efforts to improve performance and affordability* by moving from Component and platform centric capabilities to networked, enterprise architectures that support rapid adoption, integration, and modular refreshment of technologies.

Appendix: Implementation Guidance

DoD CIO, as the Principal Staff Assistant and senior advisor to the Secretary of Defense for information technology and national security systems, is responsible for developing strategy, policy, and enterprise architectures for DoD C3 systems. As such, DoD Deputy Chief Information Officer for Command, Control, and Communications (DCIO (C3)) has primary responsibility for implementing the *DoD C3 Modernization Strategy*.

The DoD CIO works closely with other DoD and OSD Components to fulfill its responsibilities. As appropriate, the DCIO (C3) will collaborate and coordinate with the Office of the OUSD(A&S), OUSD(R&E), the Military Departments, the Joint Staff, and the Combatant Commands to successfully execute this strategy.

The purpose of this appendix is to provide high-level guidance to modernize the Department's C3 systems and infrastructure. It outlines priority activities the Department must pursue to achieve the goals of this strategy as well as those of the 2018 NDS and the *DoD Digital Modernization Strategy*. It is not comprehensive of all C3 modernization activities required nor does it direct fiscal programming. Rather, it will help guide follow-on governance body assessments and analytic efforts to inform Military Department POMs and Program Budget Review (PBR) decisions.

DCIO (C3) will work through the Command, Control, and Communications Leadership Board (C3LB) and other senior governance bodies to execute the following Department-wide implementation efforts:

Goal 1: Develop and Implement Agile Electromagnetic Spectrum Operations

LOE 1.1 – Enhance EMS data collection and aggregation to provide accurate, relevant, discoverable, understandable, and trusted information.

- Migrate spectrum applications to cloud
- Improve cloud data fusion/integration
- Improve cloud-based data analytics

LOE 1.2 – Develop AI-enabled data analytics to enhance decision-making and capabilities for EMSO.

- Implement initial cloud based data analytics
- Implement spectrum decision support capability

LOE 1.3 – Improve EMS understanding and situational awareness capabilities to characterize and mitigate the risks from congested and contested EMOE.

- Modernize spectrum applications
- Cloud-based Spectrum Situational Awareness initial operational capability

LOE 1.4 – Develop cognitive, dynamic, spectrum access and sharing capabilities to provide the warfighter reliable EMS access when and where needed.

- Modernize spectrum applications

LOE 1.5 – Implement standardized automation interfaces to allow spectrum dependent systems to accept, avoid, reduce, or transfer spectrum access risks dynamically as they occur.

- Publish Electromagnetic Spectrum Enterprise Architecture

Goal 2: Enhance the Delivery, Diversity, and Resilience of PNT Information

LOE 2.1 – Implement a modular open-system approach to integration of DoD PNT Enterprise capabilities to enable maximum flexibility and unpredictability in responding to the evolving NAVWAR threat environment.

LOE 2.2 – Field modernized PNT capabilities.

LOE 2.3 – Develop NAVWAR partnerships with allies and coalition partners.

LOE 2.4 – Cooperate closely with other federal departments and agencies regarding civilian use and modernization of GPS for peaceful purposes and facilitating access to appropriate levels of GPS services to meet requirements for homeland security purposes.

Implementation – Governance is a core tenet of the DoD PNT Enterprise. To succeed, the DoD PNT Enterprise requires organizations across DoD to work together to develop the operational concepts necessary to implement and employ PNT capabilities to achieve integrated, seamless PNT-enabled NAVWAR Operations in support of military missions. Policy guidance and compliance issuances are at the heart of the governance process. DoD 4650 family of directives, instructions, and manuals guide the implementation of the DoD PNT Enterprise throughout the Department. Additionally, implementation is informed by a governance process conducted through the DoD PNT Enterprise Oversight Council structure, established in DoD Directive (DoDD) 4650.05, *Positioning, Navigation, and Timing (PNT)*. The process is iterative, driven by the annual DoD budget cycle, through which PNT threats are evaluated, gaps are determined, capabilities are developed, and applications are implemented to ensure NAVWAR compliance for all elements of the DoD Joint Force structure and supporting information systems. As Secretariat for the DoD PNT Enterprise Oversight Council (OC) and as Chair of the DoD PNT Executive Management Board (EMB), the DoD CIO is the Department focal point for oversight of all PNT Enterprise actions affecting both internal and external Departmental equities. Implementation actions assigned through the OC structure reflect Component responsibilities included in the DoDD 4650.05 family of issuances. Execution of implementation actions will be tracked through regular meetings of the DoD PNT Enterprise OC and EMB.

Goal 3: Strengthen National Leadership Command Capability

LOE 3.1 – Sustain secure senior leadership and continuity communications.

- Execute Plan of Action and Milestones developed for holistic modernization plan including enterprise analysis of all communications, networks and facilities

LOE 3.2 – Modernize senior leadership and continuity communications that are secure, resilient, and reliable.

- Enterprise analysis of communications and facilities, taking account of the investment being made across the DoD and leveraging the fully-networked capabilities being developed

LOE 3.3 – Ensure the cybersecurity of senior leadership and continuity communications.

- NLCC security operations center for cyber-defense, network, facility and infrastructure monitoring

LOE 3.4 – Ensure DoD C3 systems are interoperable with and capable of information sharing between NLCC and the broader National Security and Emergency Preparedness capabilities including interagency, State, local, tribal and territorial governments.

- Finalization of equipment installations for interoperability

Goal 4: Provide Integrated and Interoperable Beyond-Line-of-Sight (BLOS) Communications Capabilities

LOE 4.1 – Establish and continuously monitor strategy, policies, procedures, and other elements of the DoD SATCOM governance framework.

- Conduct SATCOM Systems Engineering Groups and two SATCOM Synchronization and Integration Work Shops (SSIWS) and up-channel decisions to the C3LB
- Utilize the DoD CIO Budget Certification Process via developing CPG directed at influencing Military Department investment in SATCOM capabilities
- DoD CIO attend the Annual Narrowband, Wideband, and SATCOM Working Groups hosted by U.S. Space Command J36
- Amend charter of SATCOM Systems Engineering Group to change the operational chair from U.S. Strategic Command to USSPACECOM, and add USCYBERCOM and USSF as members, and align under the C3LB
- Update and publish DoDI 8420.02, *DoD Satellite Communications*, to reflect changes in Department organization and responsibilities since originally issued in 2016
- Develop DoD SATCOM Strategic Implementation Plan

LOE 4.2 – Conduct requirements-informed architecture planning activities to establish a responsive, resilient, integrated DoD SATCOM enterprise.

- DoD CIO develop the SATCOM Terminal RA and submit for Joint Information Environment (JIE) Executive Committee (EXCOM) approval
- DoD CIO develop the SATCOM Gateway RA and submit for JIE EXCOM approval
- DoD CIO and DISA Complete the SATCOM Gateway Optimization and Resiliency Study
- DISA update the SATCOM Gateway Interoperability and Integration Execution Plan

- DoD CIO and USSF ensure SATCOM reference and solution architectures are aligned with the DoDIN Transport Optimization Plan
- Participate in the upcoming Narrowband SATCOM Communications Services (NSCS) AoA and provide input and analysis on ground and terminal segments of the capability
- Oversee future wideband SATCOM capabilities in accordance with the recommendations provided in the Wideband Communications Services (WCS) AoA to ensure access to cloud-based infrastructure

LOE 4.3 – Expand SATCOM cooperation and integration with Allies and International Partners.

- DoD CIO continue providing chairmanship of the NATO SATCOM Capability Area Team (CAT) on an annual basis
- Provide Future NATO SATCOM Services (FNS) as part of the Quadrilateral Consortium to NATO
- Establish Wideband Global SATCOM (WGS) resource sharing with Australia as part of the capabilities at the Combined Communications Gateway Geraldton (C2G2)
- Expand allied participation in the WGS system in coordination with the SAF/IA team
- Complete Mobile User Objective System (MUOS) release to Canada in coordination with the U.S. Navy
- Expand release of MUOS to Five Eyes partners

LOE 4.4 – Acquire and field modernized DoD SATCOM capabilities for delivery of information services to the tactical edge.

- Integrate commercial SATCOM managed services as part of an overall “Hybrid” SATCOM architecture
- Integrate SATCOM Operational Management and Situational Awareness Tool (SOMSAT) into the SATCOM Integrated Operations Division’s SATCOM Common Operational Picture (COP)
- Field Protected Tactical Waveform (PTW) capable modems to support Protected Tactical Enterprise Service (PTES) capabilities over WGS and Commercial Satellite Communications (SATCOM)
- Deliver and Integrate future MUOS satellites for life cycle extension of the MUOS constellation
- Mature PTW and PTES Management functions to support the Protected Tactical SATCOM (PTS) constellation capabilities
- Deliver and Integrate WGS satellite #11
- Deliver and Integrate an Enterprise Management and Control capability for seamless SATCOM delivery across various SATCOM systems to the warfighter

LOE 4.5 – Conduct Informed and responsive DoD SATCOM resource management.

- Implement SATCOM COP based on available situational information

- Integrate SOMSAT into SATCOM COP

LOE 4.6 – Develop and deliver advanced BLOS capabilities for SATCOM-denied environments.

- Expand the use of innovative solutions to BLOS throughput shortfalls
- Support research, development, and transition of advanced BLOS technologies
- Modernize the High Frequency Global Communication System (HFGCS) ground system to incorporate digital adaptive beamforming techniques, new waveforms, networking and Automatic Link Establishment techniques and similarly modernize HF-equipped forces
- Leverage other High Frequency systems such as Over The Horizon Radars
- Field modernized HF waveform

Goal 5: Accelerate and Synchronize Fielding of Modernized Tactical Communications Systems

LOE 5.1 – Mature tactical communications enterprise governance to guide fielding decisions and synchronize Military Department efforts.

- Stand-up and formalize the C3LB as the Senior Leader governance forum for tactical communications
- Develop charter and reestablish the Radio & COMSEC Strategy Working Group as the TCSSG as a subordinate working group to the C3LB

LOE 5.2 – Develop and enforce policies and standards to improve interoperability and reduce tactical grid complexity while enhancing resilience.

- Update DoDI 4630.09, Communication Waveform Management and Standardization
- Develop assessment and testing processes for non-developmental and commercial-off-the-shelf waveforms to better address interoperability, security, and affordability of waveforms for which DoD does not own intellectual property rights
- Develop Second Generation Anti-jam Tactical UHF Radio for NATO (SATURN) v3 U.S. military standard compatible with NATO specification
- Establish reference implementations for all DoD core C2 waveforms

LOE 5.3 – Develop and publish approved joint tactical communications architectures and modernization roadmaps to enhance secure, real time/near real time tactical communications with joint, allied, coalition, and partner forces.

- Develop, staff, and approve tactical communications roadmaps
- Transition RCMP to an on-line Tactical Communications Modernization Plan
- Develop, staff, and approve tactical communications architectures
- Implement Joint Tactical Networking Center Modular Radio Architecture Framework

LOE 5.4 – Sustain and modernize tactical communications network capabilities by rapidly integrating modern communications technologies to improve the capability and survivability of DoD tactical networks.

- Develop guidance directed at influencing Military Department investments in critical tactical communications capabilities
- Lead Service and waveform sponsors identify legacy waveforms that have prohibitive technical or cost hurdles to modernize for use in contested environments and sundown those waveforms
- Implement Tactical Radio Risk Management Framework to establish a more consistent and repeatable security analysis, review, and protection process for tactical radios
- Manage DoD transition from HAVE QUICK to SATURN capability
- Manage DoD transition to Single Channel Ground and Airborne Radio System (SINCGARS) v3.1
- Implement Cryptographic Modernization Program Mod 1 (CM1) programs over the FYDP for achieving near-term C3 modernization; and longer term, of C3 Modernization staying in alignment with Crypto Mod 2 (CM2), and the NSA Cryptography Roadmap
- Field Link-16 advanced capabilities

Goal 6: Fully Establish and Implement a Public Safety Communications (PSC) Ecosystem

LOE 6.1 – Develop DoD policy and apply governance.

- Assign DISA executive agent responsibilities for PSC IT architecture implementation
- Issue DoD PSC Directive and Instruction
- Charter PSC Senior Steering Group to begin collective oversight of initiatives and implementation

LOE 6.2 – Assess and mitigate capability gaps.

- Army will conduct a Department-wide assessment and baseline Enterprise Mass Warning Notification (EMWN) capabilities
- Army will provide DoD recommendations for essential tools, services, and methods
- DISA provide the DoDIN architecture requirements for State, local, tribal, and host nation interoperability
- Achieve DoD EMWN Initial Operational Capability and Fully Operational Capability respectively

LOE 6.3 – Synchronize DoD budgeting, POM, and spending.

- Establish a PSC focused program element across the Future Years Defense Program (FYDP)
- Align and plan the PSC DoD budget requirements to affect the POM22

LOE 6.4 – Develop active partnerships and engage with industry.

- DoD PSC community establish State, local, tribal, host nation, and interagency partnerships though memorandum of agreements (MOA)
- Determine DoD metrics for professional collaboration, industry interaction, exercise participation, and certifications of DoD Public Safety Answering Point (PSAP) dispatch operators and managers

Goal 7: Create an Environment to Develop 5G Infrastructure Rapidly and Leverage Non-U.S. 5G Networks

LOE 7.1 – Identify additional spectrum for 5G.

- Contribute to finalizing DoD 5G Standards Engagement Plan
- Develop radar/5G spectrum sharing testbed

LOE 7.2 – Harmonize 5G spectrum across the globe.

- Coordinate 5G spectrum harmonization work with international standards bodies

LOE 7.3 – Develop 5G standards, spectrum, and cybersecurity policy.

- Continue ongoing work coordination with 5G international standards bodies
- Develop 5G-related cybersecurity policy, standards, and guidelines

LOE 7.4 – Accelerate DoD's adoption of 5G technology.

- Develop dual-use application prototypes in such areas as mission planning, depot operations, global asset/supply chain management, and smart ports/bases
- Execute DoD-focused networking prototypes to expand the utility of 5G commercial networks for DoD missions
- Demonstrate the ability to "operate through" using dynamic spectrum utilization and controlled exploitation of 5G network security architectures and red-teaming
- Execute at-scale 5G experiments at approximately 12 DoD sites
- Collaborate with Joint Staff J6 Deputy Directorate for C5 Integration to demonstrate the mission-based interoperability of 5G with other networks and waveforms

Goal 8: Provide Resilient and Responsive Command and Control (C2) Capabilities

LOE 8.1 – Implement the JADC2 concept.

- Support JADC2 CFT to promote concept development, joint experimentation and demonstrations to evolve joint C2 capabilities
- Ensure development and implementation of common standards and computing platforms to enable application development and reuse across the force

- Enable and allow Federally-Funded Research and Development Center expertise in the development of common standards/architectures to support JADC2 concepts

LOE 8.2 – Modernize command and control systems.

- Modernize C2 capabilities for joint situational awareness and access to intelligence data and tools through delivery of an enhanced version of Global Command and Control System – Joint (GCCS-J) and eventual transition to an enterprise-hosted, cloud-based deployment model
- Provide modernized air operations C2 capabilities needed to create and execute the air tasking order (ATO) through development of new cloud-based software; create the conditions to deprecate the legacy Theater Battle Management Core System (TBMCS)
- Implement enhanced joint crisis action planning and force projection capabilities through delivery of the Joint Planning and Execution Service (JPES) as a replacement for the legacy Joint Operational Planning and Execution Systems (JOPES)
- Collaborate with U.S. Transportation Command/Joint Enabling Capabilities Command (JECC) to develop a business case and corresponding acquisition and funding strategy to replace the legacy Deployable Joint Command and Control (DJC2) system
- Collaborate with the Joint Staff J6 Deputy Directorate for C5 Integration to demonstrate mission-based multi-domain multi-classification and resilient C5 capabilities
- Adopt a single modern and efficient machine-to-machine C2 messaging standard

LOE 8.3 – Implement information-sharing standards.

- Implement the National Information Exchange Model (NIEM) as a preferred information exchange specification in GCCS-J and interfacing systems to improve interoperability and understandability at the data objective level
- Adopt modernized interface standards to transition from point to point interfaces to data provided by web-services

LOE 8.4 – Promote software agility and increased cybersecurity.

- Pilot agile software development methods in key joint C2 programs (e.g., GCCS-J, Air Operations Center Weapon System Block 20) to reduce the time to field new capabilities to the joint warfighter, consistent with National Defense Authorization Act direction
- Complete development of a new software acquisition pathway policy
- Participate in the OUSD(A&S)-led agile software community of practice to promote sharing of lesson learned and best business practices to improve adoption of agile software acquisition practices across all C2 programs

Goal 9: Deliver Mission Partner Environment (MPE) Capability and Services

LOE 9.1 – Establish policy and procedures for a DoD-wide MPE framework.

- Update DoDI 8110.01, *Mission Partner Environment (MPE) Information Sharing Capability Implementation*, to align MPE policy, responsibilities, and procedures with new executive agent and Principal Staff Assistant designations

LOE 9.2 – Transition from disparate legacy solutions.

- Execute Joint Interoperability Data Centricity (JIDC) joint test effort to develop, test, and evaluate tactics, techniques, and procedures to establish and utilize a data centric environment that enables Mission Commanders at the operational and tactical levels to effectively collaborate and conduct operations with coalition and multi-national partners
- Develop Mission Partner Gateway eXtended (MPGW-X) to optimize, converge, secure, and standardize connections to U.S. partners globally

LOE 9.3 – Application of interoperability compliance and assessment.

- Conduct mission-based interoperability compliance assessments capabilities to ensure information can be exchanged with whom it is required, when and where it is required, as determined by operational need and the accepted level of risk