The appearance of external hyperlinks does not constitute endorsement by the United States Department of Defense (DoD) of the linked websites, or the information, products or services contained therein. The DoD does not exercise any editorial, security, or other control over the information you may find at these locations.

October 11, 2024

DEPARTMENT OF DEFENSE

PRIVATE 5G DEPLOYMENT STRATEGY

FOREWORD

The 2022 National Defense Strategy calls for the Department of Defense (DoD) to construct an enduring foundation to secure our future military advantage. Part of the broad and deep change in how we produce and manage military capabilities requires the Department to make the optimal and appropriate technology investments. The 2024 Fulcrum DoD IT Advancement Strategy improves our digital environment and affords the Joint Force a competitive advantage in the modern battlespace by focusing on the most promising technologies and adopting enterprise systems and services. Fifth generation (5G) mobile network technologies provide capabilities that accelerate enterprise innovation, optimize services for efficiencies and improved capability, and enable Fulcrum LOE 2: modernize information networks and compute to rapidly meet mission and business needs.

Our world is changing, and the Department must accelerate adoption and implementation of 5G technology to deliver new levels of wireless mobility network performance, capabilities, and efficiencies that contribute to the warfighting capacity and lethality of the Joint Force. We must leverage emerging and advanced technologies to become more efficient, effective, automated, and sustainable. This includes a global interconnected communications network that is robust, high performing, secure, agile, and resilient—designed to accommodate scalability, rapid adaptation for war, and rapid reconstitution.

The DoD's 5G Strategy (2020) recognizes this change and highlights that the deployment of 5G capabilities and networks will be far more disruptive than those of prior generations. This Private 5G Deployment Strategy serves as an addendum to the DoD 5G Strategy and 5G Strategy Implementation Plan (2020), providing overarching guidance for deploying private 5G networks at military installations.

A key aspect to DoD's modernization effort is to leverage 5G networks, both commercial and private, to deliver ubiquitous high-speed connectivity for mobile capabilities. Commercial networks offer core 5G services to a broad range of users across densely populated portions of military installations. The Department will leverage commercial networks to the maximum extent possible; however, DoD acknowledges that under certain circumstances, commercial networks may not fulfill an installation's requirements. Private networks can augment or supplement commercial services, as they are tailored to the specific installation's mission needs, security, and military-unique capabilities.

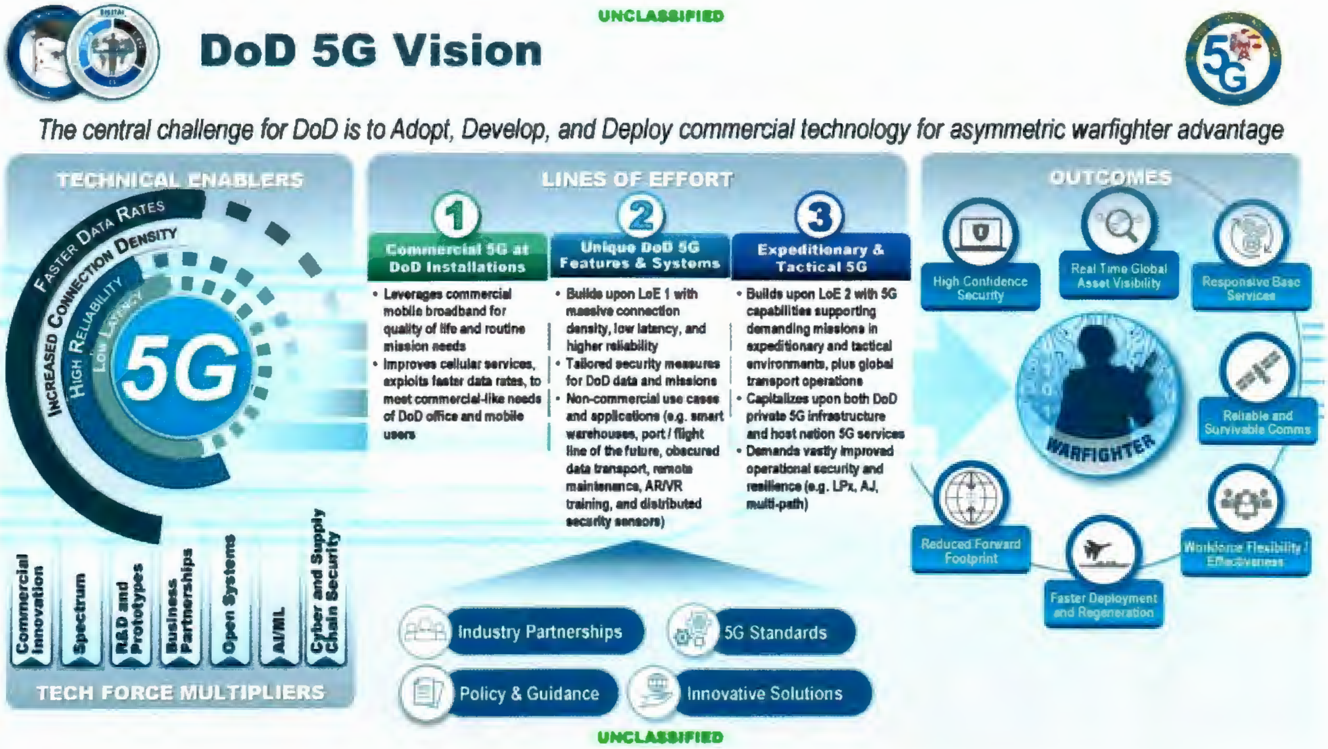
DoD's telecommunications ecosystem, services, and supporting infrastructure—which includes 5G networks—work seamlessly to streamline data access and to provide secure, universal, high-speed, high-capacity coverage. The need for high-performance connectivity will require a common approach to acquisition, development, deployment, and lifecycle support. This foundational strategy and subsequent implementation material identify key activities to drive, enable, and govern mission-focused and cost-effective solutions enabling global warfighting capabilities of the Joint Force.

Leslie A. Beavers OCT 16 2024

Leslie A. Beavers
Acting Chief Information Officer of the
Department of Defense

EXECUTIVE SUMMARY

Deploying 5G requires a unique planning approach, where the Department must not only protect against today's threats but transform the future network so that it is mission-tailored, integrated across the Joint Force, and cyber-resilient. This strategy identifies key activities to facilitate, synchronize, and govern the implementation and operation of private fifth generation (5G) networks, as defined by 3rd Generation Partnership Project (3GPP), at military installations. To fully align with DoD's 5G Vision (Figure 1), the deployment and management of 5G networks in any of the lines of effort require effective governance mechanisms to ensure successful implementation.



UNCLASSIFIED

DoD 5G Vision

The central challenge for DoD is to Adopt, Develop, and Deploy commercial technology for asymmetric warfighter advantage

LINES OF EFFORT

1 Commercial 5G at DoD Installations

- Leverages commercial mobile broadband for quality of life and routine mission needs
- Improves cellular services, exploits faster data rates, to meet commercial-like needs of DoD office and mobile users

2 Unique DoD 5G Features & Systems

- Builds upon LoE 1 with massive connection density, low latency, and higher reliability
- Tailored security measures for DoD data and missions
- Non-commercial use cases and applications (e.g. smart warehouses, port / flight line of the future, obscured data transport, remote maintenance, AR/VR training, and distributed security sensors)

3 Expeditionary & Tactical 5G

- Builds upon LoE 2 with 5G capabilities supporting demanding missions in expeditionary and tactical environments, plus global transport operations
- Capitalizes upon both DoD private 5G infrastructure and host nation 5G services
- Demands vastly improved operational security and resilience (e.g. LPx, AJ, multi-path)

UNCLASSIFIED

Figure 1 - DoD 5G Vision

This strategy provides decision-making guidance to implement a DoD private 5G network and the considerations to follow throughout the planning and acquisition process.

Strategic Objectives:

- Objective 1 – Ensure private 5G infrastructure aligns with each installation's unique mission(s).
- Objective 2 – Accelerate acquisition, development, and secure deployment of 5G.
- Objective 3 – Expand the use of an Open Radio Access Network (Open RAN) ecosystem.

The U.S. military must leverage the connectivity and advanced networking flexibility provided by 5G to operate with the speed, precision, and efficiency necessary in future engagements. This strategy ensures the Department leverages the most appropriate commercial wireless investments, standardizes modernization processes, avoids stove-piped solutions, balances mission and costs, prioritizes cybersecurity and supply chain risk management, maximizes interoperability, and strengthens the U.S. industrial base.

INTRODUCTION

The Department of Defense (DoD) must modernize military installation communications networks and telecommunications infrastructure to overcome deficiencies in capacity, scalability, agility, interoperability, and resiliency to effectively support all-domain operations of the Joint Force. 5G infrastructure will lead to increased network capacity, enhanced communications reliability, and enables fielding of diverse enterprise and mission wireless applications. The DoD and other Federal gencies are promoting 5G deployment, testing advantages and potential vulnerabilities of 5G, engaging with private-sector partners, and actively influencing industry through shared research, prototype deployment programs, policies, and standards.

This strategy builds on prior DoD guidance on deployment and use of 5G capabilities. The "DoD 5G Strategy" was developed as the Department's actions in support of the National Strategy to Secure 5G (Public Law 116-129, "Secure 5G and Beyond Act," March 23, 2020) and aligns with the National Defense Authorization Act for Fiscal Year 2020 (FY 2020), Section 254. The subsequent "DoD 5G Strategy Implementation Plan" served as an addendum to the DoD 5G Strategy and provided guidance for execution of the DoD 5G Strategy. Both documents provide the need to use "private, hybrid, and public 5G networks" in DoD global operations.

This strategy focuses on the deployment of private 5G networks on military installations and recommends the use of Open Radio Access Network (RAN) solutions, whenever possible and appropriate, and the types of private networks and the associated security and performance considerations necessary.

KEY TERMINOLOGY

Unlike mobile network services offered to the public, a private 5G network provides services to a clearly defined and approved user group. Such private networks are built for a targeted purpose with specific performance, access, and security in mind. Private networks may be owned, operated, and/or deployed by mobile network operators (MNOs), system integrators, other third parties, or the installation itself. The key distinction is that a private 5G network is only accessible to authorized users, as defined by the system owner.

Both public and private 5G networks comprise a 5G system that is made up of User Equipment (UE), a Radio Access Network (RAN), and a Core Network, all configured to support services provided by the 5G system. For the purposes of this strategy, private 5G is defined by the 3rd Generation Partnership Project (3GPP) in Technical Specification (TS) 23.501[1] as a Stand Alone Non-Public Network (NPN) that does not rely upon network functions provided by a Public Land Mobile Network (PLMN), with the caveat that private 5G networks in DoD are not likely to be strictly stand alone NPN, but could encompass some enhanced PLMN-dependent services, such as private/public network roaming or Non-Terrestrial Network access.

[1] Latest version of 3GPP TS 23.501 can be found at: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144

Open Radio Access Network (RAN) is part of the 5G architecture that is modular, uses open interfaces, and virtualizes functionality on commodity hardware through software. The Department defines Open RAN to be based on O-RAN Alliance[2] specifications and offers further technical definition through the DoD 5G Reference Architecture, currently in development with expected release of September 1, 2025.

Military installations and other facilities will be referred herein as "military installations" (or "installations"), which is a DoD site, enduring location, a group of small non-contiguous locations, or joint base that is inclusive of active and reserve components as listed in the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD (A&S)) Real Property Directorate inventory.

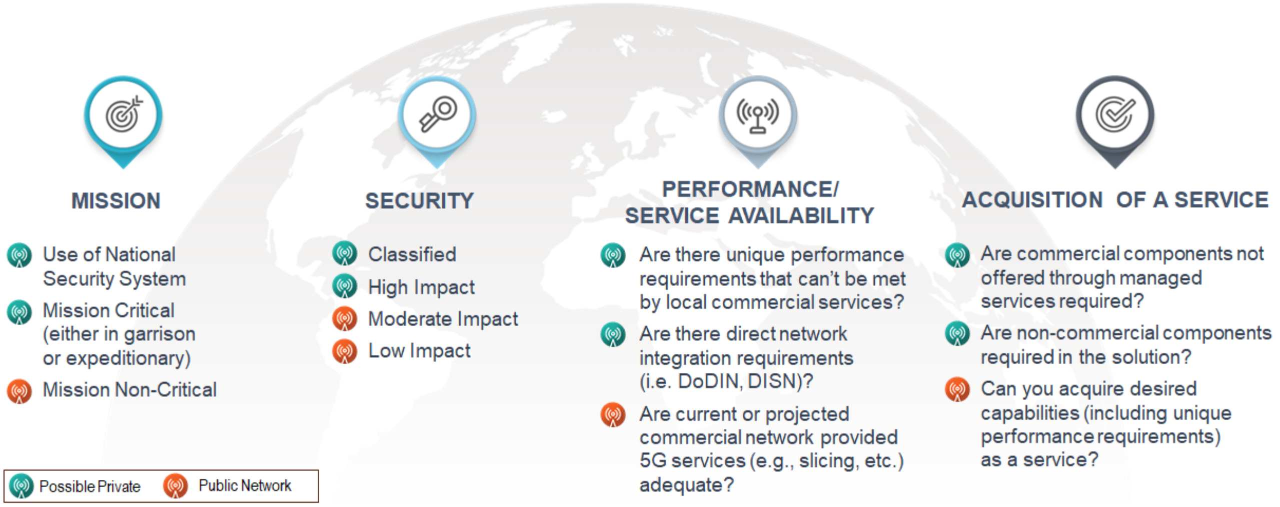
STRATEGY

This strategy provides guidance to implement a DoD private 5G network and the considerations to address when exploring the use of private 5G. As detailed below, private networks entail costs that commercial services do not incur; therefore, the Department must first fully evaluate the use of public telecommunications networks and managed services based on the operational environment before pursuing a private 5G network.

Successful use of private 5G networks for military mission applications will require consideration of mission, security, and performance/coverage requirements, as well as acquisition approach. The DoD strategy for private 5G networks at military installations will be executed across three strategic objectives detailed below.

Objective 1 – Ensure private 5G networks at military installations consider mission, security, operating environment, performance requirements, and acquisition feasibility.

- The table below summarizes the key criteria where a private network may be acceptable; while all criteria should be considered, it is possible that a single requirement could inform a decision.



MISSION

🟩 Use of National Security System
🟩 Mission Critical (either in garrison or expeditionary)
🟧 Mission Non-Critical

SECURITY

🟩 Classified
🟩 High Impact
🟧 Moderate Impact
🟧 Low Impact

PERFORMANCE/ SERVICE AVAILABILITY

🟩 Are there unique performance requirements that can't be met by local commercial services?
🟩 Are there direct network integration requirements (i.e. DoDIN, DISN)?
🟧 Are current or projected commercial network provided 5G services (e.g., slicing, etc.) adequate?

ACQUISITION OF A SERVICE

🟩 Are commercial components not offered through managed services required?
🟩 Are non-commercial components required in the solution?
🟧 Can you acquire desired capabilities (including unique performance requirements) as a service?

🟩 Possible Private 🟧 Public Network

Figure 2. Private 5G Considerations

[2] O-RAN Alliance website: https://www.o-ran.org/

- Leverage commercial services to the maximum extent practical and assess requirements to invest smartly in private 5G when needed to avoid incurring unnecessary cost.
  On a site-by-site basis, perform a technical and business case analysis (BCA) to determine whether specific mission, security, coverage, and performance requirements may only be met by private 5G. This ensures that network infrastructure is maintainable, scalable, and able to meet the changing needs of the specific military site.

Objective 2 – Accelerate acquisition, development, and secure deployment of 5G.

Enhance IT management and oversight to ensure effective use of resources and alignment with mission objective at the speed of warfare.

- Reduce delivery cycle timeline.

  Consult the 5G Acquisition Playbook to guide implementation of private 5G networks. The purpose of the 5G Acquisition Playbook is to help accelerate the adoption of 5G capabilities across the Department. It will provide essential guidance to adopt or integrate new commercial 5G capabilities into DoD missions and systems while focusing primarily on the deployment of 5G systems on or adjacent to military installations. The 5G Acquisition Playbook is one of the tools DoD CIO has developed to meet Objective #2.

- DoD Components refer to technical guidance for deployment of private 5G networks.

  Components will utilize the forthcoming DoD 5G Reference Architecture to deploy 5G systems and ancillary features and functions. The Reference Architecture will lay out the baseline implementation for DoD's use of 5G and then extend the baseline implementation to cover additional 5G features, such as Non-Terrestrial Networking, Network Slicing, Multi-Operator Core Networks (MOCN), neutral host networks, private/public network roaming, Multi-access Edge Computing (MEC), Integrated Access and Backhaul (IAB), etc.

- Increase use of common architectures, risk frameworks, and standards.

  Common infrastructure should be leveraged where feasible and appropriate. For example, military installations should consider leveraging the planned enterprise DoD 5G core network,3 rather than establishing individual dedicated 5G core networks. While certain requirements could necessitate an installation-specific 5G core network, use of the DoD 5G SA core and its attendant cyber defense capabilities will offer optimal security. An enterprise DoD 5G core network would be a dedicated 5G core with its own hardware and software, rather than relying on 5G as a service offered by commercial providers. DoD components/installations will factor in the availability of the enterprise DoD 5G Core network into their BCA as part of the decision-making process for deploying 5G on the installation.

- Private 5G networks must adhere to cybersecurity and supply chain risk management requirements.

  As with most products utilized by DoD, 5G equipment, products, and services are required to comply with DoD supply chain requirements to obtain the level of assurance from threats/risk in deployment.

[3] Pending an analysis of alternatives to determine business model, architecture, resourcing. Implementation of an enterprise DoD 5G core network would be developed and planned in consultation with the MilDeps.

These shall meet the appropriate compliance requirements, including but not limited to, FY19 NDAA Section 889, as implemented in the Federal Acquisition Regulation (FAR) part 4.21. Additionally, DoD Components must adhere to Executive Order 13873, "Securing the Information and Communications Technology and Services Supply Chain," May 15, 2019. 5G technologies, networks, devices, applications, and services must comply with DoD's cybersecurity requirements, including zero-trust principles, and supply chain risk management requirements.

- DoD Components and mission partners will adopt the Defense Information System Agency's (DISA) continuous monitoring (CM) capabilities, or a similar Cybersecurity Service Provider (CSSP) CM capability service approved by DoD CIO, for private networks.

Objective 3 – Expand the use of an Open RAN ecosystem.

Open RAN solutions offer transparent interfaces, component modularity, and a new radio layer application capability that enable greater vendor diversity, supply chain security, and operational innovation. DoD seeks to leverage Open RAN solutions where it makes mission, technical, and financial sense. To cement the value proposition, DoD will also conduct additional prototypes focused on specific DoD use cases.

- In the deployment of private 5G networks at military installations, the Military Departments (MilDeps) should incorporate Open RAN solutions in both commercial and government-owned models unless there are specific operational, technical, or business concerns that make this approach impractical or cost prohibitive.

- Develop and deploy Open RAN prototypes that take specific advantage of the RAN Intelligent Controller (RIC).

  Further experimentation with DoD specific use cases for RIC applications can unleash innovation at the 5G radio layer for flexible networks, spectrum agility, and spectrum and device management at scale. Each Service's development and deployments of Open RAN prototypes will lay the foundation for novel and innovative use of RIC applications critical to motivating and informing the expanded use of private 5G across the Department.

Implementation

Consistent with Section 224(f) of the National Defense Authorization Act for Fiscal Year 2021, each MILDEP retains responsibility for decisions relating to the procurement of 5G for that department. Accordingly, DoD CIO will provide a DoD 5G Reference Architecture and a DoD 5G Acquisition Playbook to inform the MILDEPs' implementation of this strategy for their respective installations. DoD CIO's 5G Cross-Functional Team (5G CFT) will convene and lead a working group with representation from the DoD Components to examine, evaluate, and make recommendations regarding:

  - A private 5G governance construct
  - A private 5G BCA template
  - Parameters to analyze alternatives for an enterprise 5G Core Network.

APPENDIX A – ACRONYMS / DEFINITIONS

Acronyms

3GPP – 3rd Generation Partnership Project

5G – Fifth-generation wireless

A&S – Acquisition and Sustainment

ATIS – Alliance for Telecommunications Industry Solutions

BCA – Business Case Analysis

C3 – Command, Control, and Communications

CBRS – Citizens Broadband Radio Service

CIO – Chief Information Officer

DDIL – denied, degraded, intermittent, and limited

DISA – Defense Information Systems Agency

DISN – Defense Information Systems Network

DODIN – Department of Defense Information Network

DON – Department of Navy

eMBB – enhanced Mobile Broadband

EMS – Electromagnetic Spectrum

FAR – Federal Acquisition Regulations

IoT – Internet of Things

LoE – Line of Effort

mMTC – massive Machine Type Communications

MNO – Mobile Network Operators

NDAA – National Defense Authorization Act

NPN – Non-public network

NTIA – National Telecommunications and Information Administration

OCONUS – Outside CONUS

O-RAN – O-RAN Alliance

OUSD – Office of the Undersecretary of Defense

PLMN – Public Land Mobile Network

PNI-NPN – Public Network Integrated – Non-Public Network

RAN – Radio Access Network

R&E – Research and Engineering

RIC – RAN Intelligent Controller

SCRM – Supply Chain Risk Management

SPWG – Secure Profile Working Group

TS – Technical Specification

UE – User Equipment

URLLC – Ultra Reliable Low Latency Communications

Definitions

To keep pace with industry, most terms in this strategy are defined by a 3GPP TS and are referenced accordingly. Terms used in this strategy that are not defined by 3GPP are associated to the applicable term or defined separately.

Hybrid network – See public network integrated NPN (PNI-NPN) [TS 2350.01]

Non-public network (NPN) – A network that is intended for non-public use. [TS 22.261]

Private network – An isolated network deployment that does not interact with a public network. [TS 22.261]. See also stand-alone non-public network.

Public network integrated NPN (PNI-NPN) – A non-public network deployed with the support of a PLMN. [TS 2350.01]

Stand-alone non-public network – A non-public network not relying on network functions provided by a PLMN. [TS 2350.01]