USD (R&E)

5G FutureG Initiative Overview

Mr. Larry Hencshel
Director of International 5G
Office of the Under Secretary of Defense for Research & Engineering

DoD 5G – Future G Initiative - Overview

Innovate, accelerate, and deploy dual-use next generation wireless technologies to master the connectivity of everything

Objectives:

- **5G Prototyping & Experimentation**
  - To accelerate development and deployment for military operations
  - Eight military use cases at fourteen military installations

Smart Warehouse

Spectrum Sharing (and Coexistence)

AR/VR (Remote Training)

Next Gen Range (Future Training Ranges)

EABO Wireless Comms (Expeditionary Advanced Base Ops)

Telementoring (AR/VR Guided Medicine)

Emergency Services (Pierside Communications)

- **Securing 5G**
  - Enable military operations over untrusted networks
  - Understand and mitigate the risks and vulnerabilities of 5G for military ops
- **Future G**
  - Create NextG technologies to influence future wireless standards
  - Invest in NextG to help US regain leadership in wireless technologies
- **Reinforce these thrusts with interagency and international partnerships**

DoD 5G Strategy & Activities

Promote Technology Development

- **Hosting 5G Demonstrations** – Prototype and experiment from nets to apps
- **RF Technology** – Leverage US millimeter wave expertise
- **Dynamic Spectrum Sharing** – Evaluate sharing for key Department of Defense (DoD) systems
- **Open Architecture & Virtualization** – New architectures for innovation & security
- **Workforce Development** – DoD expertise for 5G and beyond

Assess, Mitigate, and Operate Through 5G Vulnerabilities

- **Threat Intelligence** – Understanding adversaries' capabilities
- **Minimizing 5G Infrastructure Risks** – Mitigate supply chain vulnerabilities
- **Operate Through** – Use 5G globally despite adversary capabilities
- **5G Security Assessments** – Discover, assess, and mitigate vulnerabilities
- **Cybersecurity and Zero-Trust** – New architectures for in-depth security

Influence 5G Standards and Policies

- **Standards Bodies** – DoD-wide engagement w/ 5G organizations, e.g., 3GPP
- **Advanced Spectrum Management** – Modernize policies to be dynamic
- **5G-Enabled Concepts of Operation** – Modernize DoD telecom use
- **Technology Control Measures** – Review foreign investments, export controls

Engage Partners

- **International Allies and Partners** – Supply chains, assessments, experiments
- **Industry Engagement** – Engage with 5G industry ecosystem
- **Congressional Engagement** – Strengthen incentives, fix open market distortions

5G FutureG Initiative Roadmap

Fiscal Years → to	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031+
5G Prototypes & Experimentation	**Prototypes and Experiments**									
	Testbeds at 14 Locations				*Transitions to PORs and Services*					
		Military Applications for 20+ Use Cases								
			Wireless Network Enhancements							
Securing 5G	**Assess 5G Threats**									
	Non-secure Testbed		*Prototype Assessments*							
	Ensure 5G Operations									
	Tailored Network		*Black Box Network*							
			Cooperative Network		*Transitions to CCMDs*					
Innovate Future G	**Explore FutureG Technologies**									
	International Standards				*Dynamic Spectrum Management*					
		Mobile Distributed MIMO				*Transitions*				
			Integrated Tactical Networks							
Seedlings and Studies	**Cross-cutting Research and Engineering**									
	NTIA Open 5G Challenge		Resilient Open-Source for DoD		NTN		Enhanced virtualization		5G Security HW	
		5G Radar Coexistence		*5G compatible expeditionary comms*				*Transitions: to main lines of effort and end users*		
		5G in the EW kill chain		*Network Sharing Frameworks*						

LEGEND

5G to FutureG Enabled Capabilities

Key Milestones

Future 5G R&E Needs

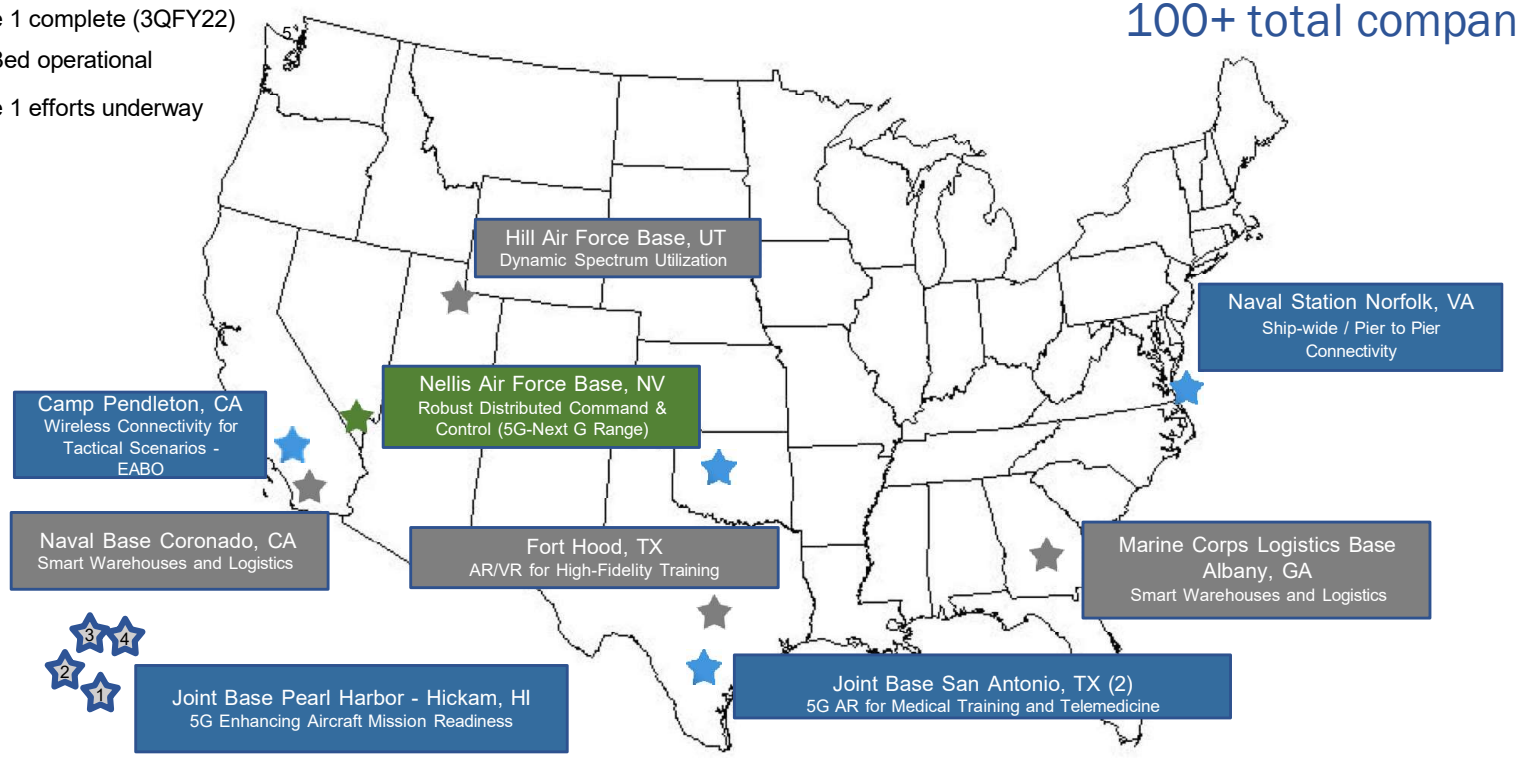
- Operational Use Cases for FutureG
- Larger Scale and Capacity Testbeds

Major Investments to Enable Fielding 5G to FutureG Capabilities

Tranche Prototyping and Experimentation

Contracts awarded to date: 65 awards and 100+ total companies

Tranche 1	Phase 1 complete (3QFY22)
Tranche 1.5	Test Bed operational
Tranche 2	Phase 1 efforts underway



Tranche Prototyping and Experimentation Overview

Three Years, Three Phases, Three Elements

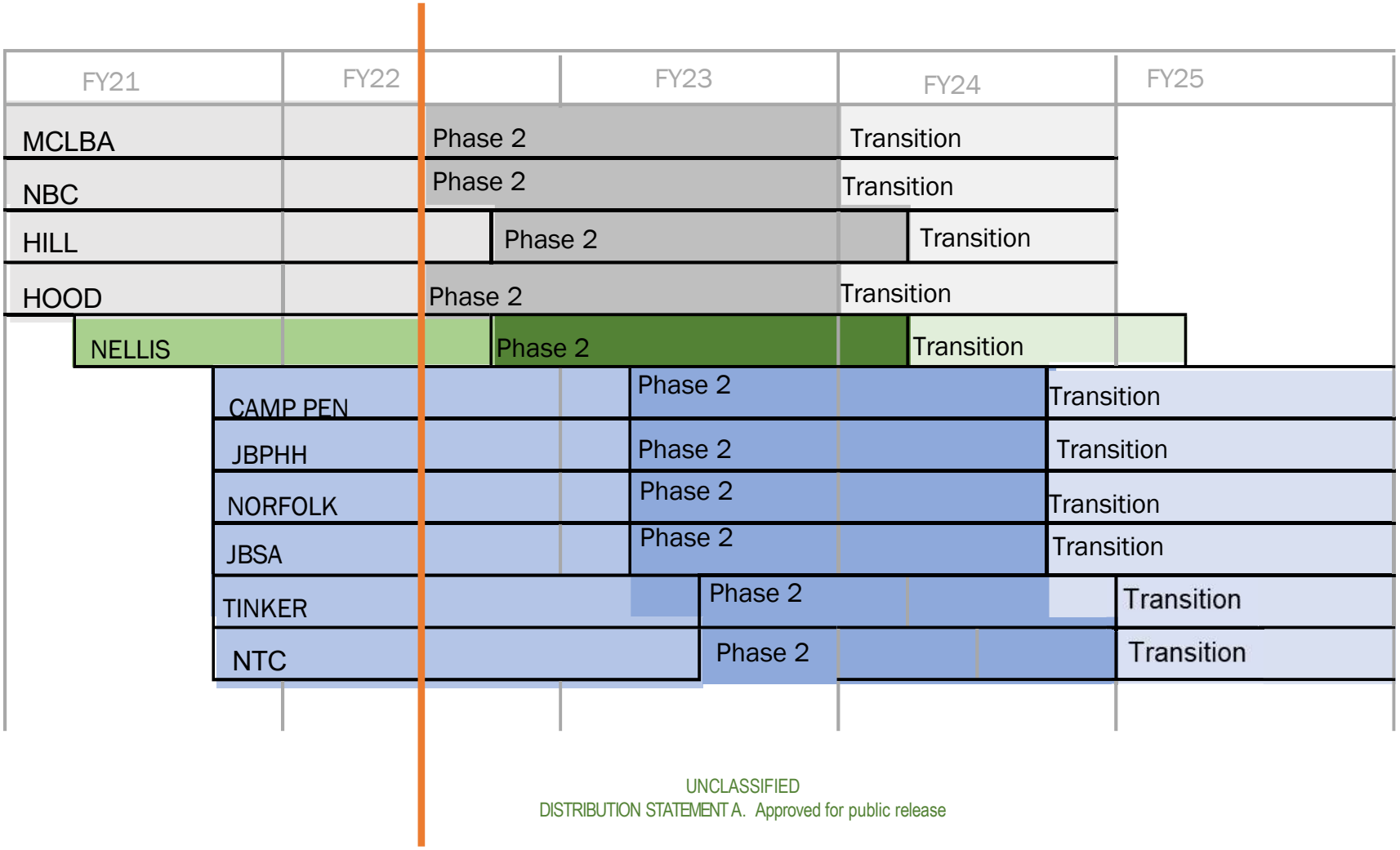
Testbed, Applications, Enhancements

Primary Objectives

- **Establish 5G Rapid Prototyping/Fielding Program for Transition into Operational Use**
  - Secure, trusted supply chain
  - Pre-approved, secure Bills of Material
  - Operationally useful, value-added applications and enhancements
- **Provide the Foundation for 5G Capability Integration into the DoD Enterprise**
  - Characterize the edges of 5G capabilities and identify capability gaps
  - Contribute to emerging 5G standards for DoD and Commercial use
  - Foster and promote Commercial development of 5G technologies

Competition → Crisis → Contested → Conflict

Tranche Prototyping and Experimentation Phased Transitions



Operating Through Existing Infrastructure

Build Your Own Infrastructure

Capability to Build Bridges

AND

Operate Through Existing Infrastructure

Make Use of Existing Bridges

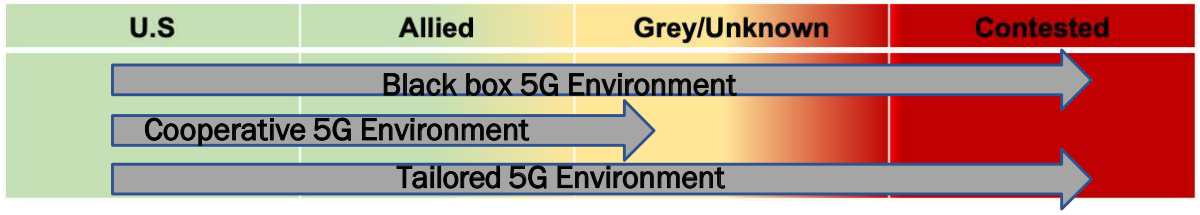
Capability to Build Comm Infrastructure

AND

Make Use of Existing Comm Infrastructure

Operate Through Environments

- **"Black box" 5G Network – Treated as an Unreliable Bit Pipe**
  - Deploy security at end devices & connect networks via untrusted bit pipe
  - Applicable to scenarios where DoD leverages indigenous infrastructure as a user
- **Cooperative Commercial/Private 5G – Provider will Work with DoD on Security**
  - Work with provider to augment some combination of RAN/MEC/CORE
  - Work within the commercial environment to the benefit of commercial provider
  - Applicable to scenarios where DoD works with indigenous infrastructure as a partner
- **Security Enhancements for a Tailored Environment**
  - Full control over code and components
  - Introduce changes to the RAN/MEC/CORE without commercial 5G constraints
  - Applicable to future scenarios where DoD has developed its own 5G capabilities



Zero Trust and Operate Through

- **Perimeter Defense Techniques are Ineffective for Operate Through**
  - Perimeter defense aims to keep adversary out of the secure system (castle and moat)
  - Lack a well-defined perimeter when operating through commercial 5G network
  - Underlying network may contain untrusted components
- **Zero Trust Introduces *Key Principles* Including**
  - Continuous monitoring to detect malfunction or misbehavior
  - Dynamic authentication and authorization
  - Segmentation (micro-perimeters)
  - Push security (e.g. encryption, access control) close to the end systems
- **Zero Trust Can *Enhance* Availability**
  - Extend zero trust concept to paths as well as devices
  - Multi-path routing and dynamic spectrum usage ensure available

Zero Trust Architecture Promising For Operate Through

Operate Through Projects

- **Diverse Projects Match Diverse "Operate Through" Challenges**
  - "Black box", cooperative, and tailored network environments
  - Modify end devices (UEs) and augment 5G networks (RAN, MEC, Core)
  - Always apply Zero Trust Principles
- **Operational Focused Efforts**
  - Driven by Combatant Command (CCMD) requirements and use cases
  - Clear user, demonstration, evaluation, and path to operations
- **Solicitations to Industry**
  - Challenges driven by combination of CCMD needs and 5G tech advances
  - Typically use Other Transaction Authority (OTA) open calls
- **Interagency and International Collaboration**
  - Work with groups such as North Atlantic Treaty Organization (NATO), Office Of Naval Research (ONR), Department of homeland Security (DHS)and others on common 5G interests

Innovate Beyond 5G (B5G) Summary

Commercial Wireless

Strategy

B5G TECHNOLOGY FRONTIERS

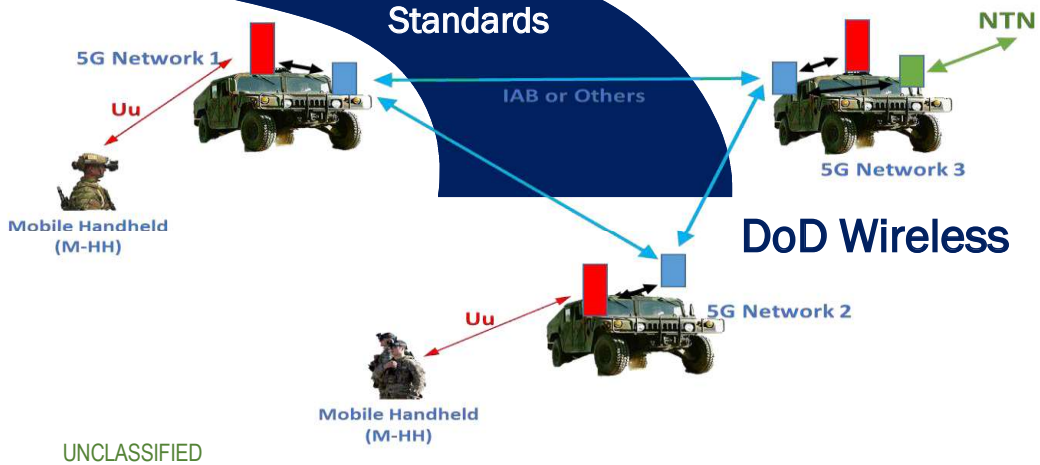
- Distributed Mobile MIMO
- Terrestrial - non Terrestrial Integration
- Multi-band, Multi-rate Operation
- Dynamic Spectrum Management
- Autonomy & Intelligence
- Network Softwarization & Virtualization

Implementation Plan

B5G STANDARDS

- Use Case - Tech Specs, Gap Analysis (5G Secure Profile Working Group, MITRE)
- 3GPP Study Items (MITRE, NTIA, National Spectrum Consortium, Alliance for Telecommunications Industry Solutions (ATIS))
- Spectrum Sharing (DoD Chief Information Officer (CIO), Defense Information Systems Agency (DISA))

Standards



International Engagement

- **Objectives**
  - Strengthen existing science and technology (S&T) relationships with allies and partners that lead to common standards, interoperable technologies and advanced 5G and FutureG technologies
  - Identify and advance 5G partnering opportunities
  - Engage international partners to advance 5G/FutureG technology
  - Amplify, align, and enable synchronized engagement for 5G and Future G
- **International Engagement**
  - **European Region**: United Kingdom, North Atlantic Treaty Organization (NATO) Multinational 5G (MN5G), NATO Collaborative Cyber Defense Centre of Excellence (CCDCOE), Estonia, and Latvia
  - **Indo-Pacific Region**: Republic of Korea (ROK), Quadrilateral Security Dialogue, and Five Eyes

Open 5G Activities

- **Exploring Open 5G with interagency partners**
  - Open Interfaces (e.g. Open RAN) , not necessarily open source
  - The 5G Challenge in collaboration with National Telecommunications and Information Administration (NTIA)
    - NTIA issued Notice of Inquiry (NOI) in January, responses currently being evaluated, aiming for solicitation in 1Q FY22
    - Challenge published April 06, 2022
  - Enable end-to-end experimentation aligned to DoD CONOPs
- **DARPA and OUSD(R&E) collaborative project**
  - Multisite Open Programmable Secure 5G (OPS-5G) Joint Independent Testing Option (MOJITO)
  - Testing at NIWC PAC (Naval information warfare center) and multiple DoD 5G sites

DoD 5G Summary

The 5G Initiative is moving out smartly to meet its major objectives.

Lessons learned from initial procurements (use of OTAs and purchasing leading-edge tech) are being applied to expedite and clarify later procurements.

OUSD is making a concerted effort to recognize and address the global needs of the Combatant Commands and the Services.

Glossary

- DOD: Department of Defense
- 5G: Fifth Generation Telecommunications
- CCMD: Combatant Command
- ONR: Office of Naval Research
- DHS: Department of Homeland Security
- NTIA: National Telecommunications and Information Administration
- NIWC PAC: Naval Information Warfare Center
- NATO: North Atlantic Treaty Organization