DEPARTMENT OF DEFENSE
5G STRATEGY IMPLEMENTATION PLAN

ADVANCING 5G TECHNOLOGY & APPLICATIONS
SECURING 5G CAPABILITIES

IN RESPONSE TO PUBLIC LAW 116-92, SECTION 254, PAGE 1287-1288, OF THE NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2020

2020

The estimated cost of this report or study for the Department of Defense is approximately $10,000 in Fiscal Years 2020 - 2021. This includes $230 in expenses and $9,970 in DoD labor.
Generated on 2020Dec11 RefID: 3-1765696

DISTRIBUTION STATEMENT A. Approved for public release.

APPROVED BY SECRETARY OF DEFENSE

December 15, 2020

INTRODUCTION

As noted in the Department of Defense 5G Strategy,[1] "5G is a critical strategic technology: those nations that master advanced communications technologies and ubiquitous connectivity will have a long-term economic and military advantage." The DoD 5G Strategy provides the DoD 5G approach in support of the National Strategy to Secure 5G[2] and the National Defense Authorization Act for Fiscal Year (FY) 2020, Section 254. This document serves as an addendum to the DoD 5G Strategy and provides additional detail regarding how the DoD 5G Strategy will be implemented throughout the Department.

5G is important to DoD because it offers higher performance and additional capabilities, particularly for data-driven applications and for machine-to-machine communication. These capabilities will become the foundation for a new networked way of war that brings together sensors and machines that will revolutionize the battlespace and the logistics and support functions behind the front lines. DoD must have access to a 5G defense industrial base that provides trustworthy 5G technologies.

Compared to earlier generations of wireless technology, 5G provides many more features that can be customized for specific applications, for example to meet the performance or security requirements of an application. Further, commercial applications and technologies are becoming increasingly aligned with DoD needs. Because of that, DoD has an opportunity to become an early adopter of 5G applications, which helps U.S. industry move more quickly in development and maturing those applications as well as the underlying 5G ecosystem. This also allows DoD to influence the development of particular applications and technologies to better align with DoD needs. As importantly, this approach provides an opportunity for DoD to address its unique security needs as well as secure operations within the global 5G ecosystem.

The DoD 5G Strategy and this implementation plan provide a roadmap for addressing the technology, security, standards and policy, and partnering aspects of how DoD can use and advance 5G networks and applications.

IMPLEMENTING THE 5G LINES OF EFFORT

The Department of Defense 5G Strategy identified the following as the necessary lines of effort to achieve the key DoD goals with respect to 5G:

1. Promote technology development,
2. Assess, mitigate, and operate through 5G vulnerabilities,
3. Influence 5G standards and policies, and
4. Engage partners.

This implementation plan describes the individual components of these lines of effort and how they are being implemented by DoD.

1. PROMOTE TECHNOLOGY DEVELOPMENT:

DoD will facilitate the advancement and adoption of 5G technology and identify new uses for 5G systems, subsystems, and components by promoting science, technology, research, development, testing and evaluation efforts

[1] *DoD 5G Strategy*, https://www.cto.mil/wp-content/uploads/2020/05/DoD_5G_Strategy_May_2020.pdf.

[2] *National Strategy to Secure 5G*, https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.

via unique access to testing sites, spectrum licenses, technical expertise, and resources. DoD will also work with industry and academia to support the development of critical technologies, integrate those technologies within a protected architecture, and demonstrate "transformative 5G and beyond" applications.[3]

DoD is seeking to promote 5G technology development by becoming an early adopter of 5G networks and applications, as well as by contributing to 5G technology innovation and maturation.

U.S. industry excels in its ability to deliver leading edge services and applications based on wireless network connectivity. DoD is becoming an early adopter of 5G applications and services by hosting 5G experiments and demonstrations at numerous DoD facilities. This will ensure that DoD has the ability to use the latest 5G-enabled technology solutions, while also providing early technology validation opportunities that will help U.S industry to continue to lead at the high end of the value chain.

It is also important that DoD have access to trustworthy technologies at the lower end of the value chain, specifically in the 5G Radio Access Network (RAN) and 5G Core. Through prototyping and experimentation activities, DoD is promoting the maturation of radio frequency (RF) technologies including millimeter wave systems, as well as dynamic spectrum utilization capabilities. DoD is also experimenting with networking technologies in both the RAN and 5G Core, with an emphasis on open architectures and virtualization approaches which leverage U.S. industry expertise.

Because DoD will need personnel that are proficient in 5G to support its deployment and use of 5G technologies, DoD is also investing in workforce development in collaboration with its interagency partners.

HOSTING 5G DEMONSTRATIONS

DoD will select military facilities that will serve as hosts for a series of 5G industry demonstrations beginning in FY 2020. These demonstrations will develop and test military and dual-use 5G technologies, concepts, and applications. Selected testbeds will benefit industry partners by providing large, complex environments that are suitable for testing the integration of 5G features (e.g., smart ports, supply chain management, and depot operations). Successfully demonstrated and proven products will be rapidly deployed, with follow-on acquisitions, operations, and sustainment through the appropriate organizations across DoD.

DoD has begun hosting 5G at-scale prototyping and experimentation in collaboration with industry at twelve DoD facilities.[4] At each site, a 5G network testbed is being installed, to prototype advanced 5G network technology, and to experiment with DoD use of 5G. Each site is host to at least one prototype 5G-enabled application that utilizes features of 5G to improve DoD capabilities. Each site is also host to prototyping and experimentation with advanced 5G technologies that can enhance the testbed and the application. In addition to the initial experiments being performed at each site, it is anticipated that additional experiments that use the testbeds will be performed.

These efforts are a collaborative effort across DoD, including the Services and the user communities at each facility. By actively engaging with the user community, the prototypes developed in these at-scale experiments can be transitioned to programs of record in the appropriate areas.

DoD is prototyping and evaluating 5G technologies in the following initial tranches of experiments:

- At Hill Air Force Base (AFB), the Air Force is evaluating the impact of 5G systems on airborne radars, and vice versa, in the midband spectrum, and developing techniques to dynamically utilize spectrum, enabling radars and 5G systems to coexist.
- At Naval Base San Diego, the Navy is prototyping 5G smart warehouse systems for transshipment of supplies and material through logistics depots to ships at sea.

[3] Paragraphs in italics are drawn directly from the *DoD 5G Strategy*.

[4] DoD 5G-to-Next G Initiative, https://www.5g-to-xg.org/.

- At Marine Corps Logistics Base Albany, the Marine Corps is experimenting with 5G smart warehouse technologies for vehicular storage and maintenance.
- At Joint Base Lewis-McChord and the Yakima tactical training site, the Army is experimenting with 5G technologies that enhance readiness and tactical training with the use of Augmented Reality/Virtual Reality (AR/VR) capabilities.
- At Nellis AFB, the Air Force is experimenting with resilient command and control (C2) based around nomadic and mobile distributed C2 vehicles interconnected by 5G networks.
- At Naval Station Norfolk, the Navy is evaluating the use of 5G technologies for both ship-wide and pier-side connectivity.
- At Joint Base Pearl Harbor - Hickam, the Navy, in collaboration with the Air Force, is seeking to improve aircraft readiness by using 5G for accessing aircraft maintenance data on the flight line.
- At the National Training Center in Fort Irwin the Army is focusing on mobile high-performance wireless connectivity 5G capabilities that can enable Forward Operating Command Posts to become more agile, dispersed, and difficult to detect for survivability on the modern battlefield; at Fort Hood, the Army is focusing on capabilities to enable semi-autonomous operations, remote sensing, and standoff.
- At Camp Pendleton, the Marine Corps is experimenting with the use of 5G technologies that support rapid deployment of Combat Operations Centers to improve operations tempo and resilience.
- At Joint Base San Antonio, the Army and Air Force are collaborating to provide secure, resilient and reliable 5G telemedicine applications which enables trusted care, enhances medical training opportunities, and sustains real-time functional capabilities while supporting all DoD medical mission objectives.
- At Tinker AFB, the Air Force is experimenting with5G-enhanced immersive training and education.
- At Joint Base San Antonio, in collaboration with the other DoD 5G sites, 5G Core networking technologies are being evaluated, with a focus on interoperability, security, and the applicability of 5G features to DoD needs.

Figure 1 – Example DoD 5G Applications and Experiments

There will be several outcomes from these experiments. The information and experience gained in the initial deployments of 5G at military sites will hasten DoD's use of 5G by streamlining processes such as the configuration of systems and obtaining authorization to operate (ATO) on DoD facilities. Further, the 5G applications will aid in improving the efficiency of DoD operations by modernizing common tasks in areas ranging from logistics to maintenance to health care.

RF TECHNOLOGY

DoD recognizes that truly transformational uses for "5G and beyond" capabilities will require operations across all 5G spectrum bands, including the contiguous spectrum available at high frequencies above 24 GHz in the millimeter-wave bands. The U.S. microelectronics industry excels in millimeter-wave technology, and DoD can leverage this

expertise for the development, acquisition, and fielding of millimeter-wave equipment. DoD will also support policies that foster shared co-primary Federal access, and will promote national and international standards related to millimeter-wave technologies.

DoD is investing in RF technologies that will transform military capabilities and operations by using large swaths of spectrum in the higher frequencies. These technologies will improve network capacity as well as provide DoD with better control of the spectrum.

In the millimeter wave (mmW) spectrum, DoD is helping to advance mmW technology by investing in early prototypes, particularly those that enable nomadic and mobile operations while maintaining mmW communications links between moving 5G base stations. DoD is also pursuing new concepts for spectrum utilization in the mmW bands based on advanced beamforming techniques. DoD is also investing in applications that use mmW capabilities, particularly the high capacity in bits per second enabled by the large swaths of spectrum in the mmW bands. Applications that require streaming at high data rates such as high quality video and sensor data collection are well matched to mmW capabilities. Other features of the mmW bands are also being explored, such as the ability to control RF spectrum signatures better in these bands, which makes adversary targeting more difficult and therefore improves the resilience of US forces.

In the midband and lower regions of the spectrum, DoD is experimenting with technologies that improve capacity and spectral efficiency, including polar modulation and direct waveform generation. Further, DoD continues to mature software defined radio (SDR) technologies, including hybrid systems that integrate multiple SDRs in different bands.

DoD is also focusing on beamforming technologies, which 5G has made less expensive and more widespread. Beamforming provides additional options for RF spectrum signature control, as well as better dynamic spectrum utilization.

DYNAMIC SPECTRUM UTILIZATION

Ubiquitous 5G coverage will require access to a variety of radio frequencies (RF) including those falling within the mid-band (1 GHz to 6 GHz) range. Because this spectrum is both heavily utilized by DoD and is highly sought after by the 5G industry, technologies and frameworks will be needed to share this spectrum amongst disparate users. DoD will support research, development, testing, acquisition, and fielding of systems incorporating new technologies that permit greater spectrum access while preventing harmful interference to legacy systems. DoD will develop the technologies and capabilities needed for near-real-time sharing, in order to enable military operations in congested spectrum environments.

DoD is focused on using the RF spectrum efficiently, both to provide military users of the spectrum with greater flexibility and resilience in contested spectrum environments, and to ensure that the U.S. telecommunications industry has the spectrum needed to offer the 5G capabilities that DoD and the nation require. Dynamic spectrum utilization provides the key technology foundations for these capabilities.

To ensure that DoD can continue to use its radars to sense threats both domestically and internationally, DoD is evaluating how 5G wireless networks and high-power radars can function in the same spectrum. To accomplish this, DoD is standing up a highly controlled testing environment to better understand 5G and radar spectrum dynamics that impact interference between these systems. Based on interference measurements and analyses from this testbed, dynamic spectrum utilization technologies for radar and 5G are being developed and evaluated. DoD will extend and enhance these findings to optimize spectrum utilization across a full range of military operational needs.

Other DoD efforts to improve spectrum efficiency and reduce interference include evaluating the use of AI and machine learning for spectrum resource utilization, as well as the impact of spectrum sensing and beamforming for use by military and commercial systems.

OPEN ARCHITECTURE AND VIRTUALIZATION

DoD will contribute to the development of advanced 5G network architectures. The DoD experimentation program will also inform more-secure designs for 5G core and edge systems, including Open Radio Access Networks and network slicing. The resulting open architectures, as well as virtualized networks and services, will make it easier for companies to offer 5G services, thereby spurring innovation, competition, and acquisition options. The approach will also enhance security, by providing a broader community of stakeholders that are dedicated to ensuring the overall integrity of the resulting architectures.

DoD is collaborating closely with industry to advance 5G open architecture efforts. This includes promoting open interfaces in both the RAN and 5G Core that allow for more competition and innovation, and more robust security evaluations.

DoD is evaluating multiple RAN implementations from industry in its prototyping and experimentation efforts, ranging from more traditional RAN designs to cutting-edge implementations based around open interfaces as well as open source software. A variety of hardware and software approaches are being explored, including hybrid hardware / SDR based RAN technology. The multiple system implementations are being evaluated for performance and capabilities, as well for interoperability and security.

DoD is also investigating how to utilize the transformational nature of the 5G architecture, that is, increasingly software-driven, virtualized networks. In these efforts, multiple 5G Core implementations from throughout the industry are being evaluated for interoperability and security. Because these 5G Core technologies are software-based and virtualized, they provide DoD with new flexibility for a wide range of DoD missions. For example, the use of 5G features such as network slicing and network function virtualization provide DoD with new ways to implement networks with multiple, different security and performance characteristics that are suited to specific operational needs. DoD is exploring how best to deploy these software-based networks, including cloud and mobile edge cloud architectures.

WORKFORCE DEVELOPMENT

The growth of the U.S. 5G industry requires a broad, well-trained workforce. DoD, in collaboration with academia, industry, and interagency partners, will identify the necessary skills and develop a human capital plan that leverages DoD's STEM programs and long history with university and laboratory partnerships. This approach will also extend to the next generation of talent that will be needed to develop advanced technologies for 6G and beyond.

Deployment of 5G and 6G wireless networking technology will significantly grow the economy – by transforming the workplace via digitalizing future industry (Industry 4.0). Simultaneously with DoD becoming an early adopter of these new networks and consequent promotion of dual-use technologies, planning for long-term investment in workforce development is critical. DoD will need a well-trained workforce to deploy, sustain, and use the new 5G technologies at the intersection of wireless hardware, network stack software, edge & cloud computing, and increasingly connected applications. This will require creation of a differently skilled workforce that thrives on integration of cognitive and physical systems.

DoD is collaborating with academia, industry, and interagency partners, to invest in human capital for 5G that leverages DoD's existing STEM programs in collaboration with university and laboratory partners. DoD is focusing on several areas of emphasis:

- Collaborating with academia and industry for online access and specialized content creation for 5G education & training.
- Leveraging 5G deployments/testbeds for realistic workforce training.
- Leveraging existing DoD scholarship and internship programs.
- Leveraging National Science Foundation fellowship programs, including 5G-focused activities aligned to DoD needs.

- Using existing postdoctoral programs, such as those at Federal labs, to advance 5G workforce development.
- Creating international collaborations with trusted partners for sharing of 5G testbeds for workforce development efforts.

2. ASSESS, MITIGATE, AND OPERATE THROUGH 5G VULNERABILITIES:

Given the military's need to operate within hostile and contested environments, DoD will utilize a risk-based framework to ensure the confidentiality, integrity, and availability of our 5G networks, devices, weapon systems, and applications and encourage its partners and allies to do likewise. DoD will also conduct country-specific assessments to determine how non-secure devices in ally and partner networks may affect DoD operations.

5G is on track to usher in a fundamental change in communications infrastructure across the globe and offers the promise of ubiquitous connectivity for both the military and private sector. This offers new opportunities and will create significant advantages for those organizations that can harness 5G communications.

To ensure that the DoD can continue to effectively operate anywhere and anytime, DoD is partnering with the private sector to accelerate 5G innovation so that we can rapidly take full advantage of its capabilities worldwide. The situation is analogous to making use of existing road infrastructures across the globe. A typical DoD mission does not begin by first building a new road infrastructure in the theater of operations. Of course, the existing road infrastructure may not be suitable for all DoD uses and a capability to build new infrastructure may be required. However, a first choice (and often the only choice) is to "operate through" the existing road infrastructure. Similarly, future DoD missions must operate through existing 5G network infrastructure. This infrastructure is increasingly deployed and available. Just as it is assumed DoD can operate through existing transportation infrastructures, DoD can gain significant advantages by leveraging 5G communications infrastructure and could be at significant disadvantage if it is unable to make use of the existing infrastructure.

The DoD 5G "Operate Through" concept recognizes four distinct categories of network infrastructure. In the first and least challenging category, DoD must be able to conduct sustained operations on the existing U.S. telecommunications infrastructure. In the second category, DoD operations in coalition partner countries must be able to operate through the coalition partner's national telecommunication infrastructure. In both the U.S. and coalition examples, long term bases and spontaneous operations both could benefit from access to a nation's existing telecommunications infrastructure. In a third and more challenging scenario, DoD may need to operate over "gray zone" network infrastructure that is influenced or even controlled by organizations that are not compatible with DoD mission objectives. Finally, DoD operates in contested areas. In all four environments (U.S., coalition, gray, and contested), use of the native 5G infrastructure can expand and enhance military options across the full range of military operations.

In operating through existing 5G infrastructures, one must overcome significant security vulnerabilities that can be exploited by adversaries at a global scale. Although DoD will encourage allies and partners to only deploy trustworthy 5G equipment, DoD must assume the underlying networks that provide 5G connectivity are untrusted in many scenarios. Further, the network operators may not be trusted in some environments. DoD must be able to operate through a network environment where the underlying communication equipment, the network operators, or a combination of both are adversaries. DoD is therefore focusing on techniques that ensure that U.S. forces can operate through adversary threats to 5G networks wherever we operate by leveraging dynamic spectrum access, mitigating adversary threats in the network, and fully exploiting 5G technology.

THREAT INTELLIGENCE

DoD must have a clear and comprehensive understanding of 5G threats and vulnerabilities. DoD also has concerns regarding potential adversaries' capabilities and their intent to leverage 5G technologies against U.S. interests. In addition to monitoring foreign technical developments, DoD must also understand how adversary military and intelligence forces may leverage 5G-enabled capabilities to impact operations. These evaluations must leverage U.S. allies and partner collaborations to the maximum extent possible.

5G standards incorporate new security features and this gives 5G networks the potential to operate much more securely when compared with existing commercial wireless networks. However, these features are balanced against new security concerns. Although the 5G standards incorporate more security features, these features are often left as optional and thus may not be implemented on 5G networks. Further, the degree of trust (or lack thereof) in the underlying hardware will have implications for the security of the systems using that hardware. Because of this, it will be critical to understand 5G security, focusing both on systemic vulnerabilities and adversary threats. DoD, in collaboration with its interagency partners, will accomplish this by:

- Developing techniques to identify, track, and mitigate threats and vulnerabilities that arise from different choices, configurations, and combinations of network equipment, software components, and deployment environments.
- Providing evidence-based information to regulatory agencies, standards groups, and network operators so they can make informed choices on network equipment.
- Demonstrating how vulnerabilities in underlying hardware could be exploited by an adversary to impact 5G-enabled capabilities and operations.
- Tracking how novel 5G features such as network slices and spectrum sharing are being used, and identify threats and vulnerabilities associated with these features.

Collectively, these actions provide DoD with threat intelligence on 5G networks operated by U.S. and coalition partners as well provide tools and techniques to rapidly identify threats and vulnerabilities in gray and contested network environments.

MINIMIZING 5G INFRASTRUCTURE RISKS

Risks to 5G infrastructure supply chains can be reduced and more easily managed by working with allies and partners, to ensure that suppliers adhere to stringent monitoring, inspection, physical security, operational security, and personnel-vetting standards and best practices. In accordance with Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain (May 15, 2019), DoD will not acquire, import, transfer, install, deal-in, or use 5G technologies that are produced by foreign adversaries. Moreover, DoD, in close coordination with allies and partners and industry, must develop and execute a detailed plan for supply chain risk management for this sector. The final result must support the ability of DoD to operate around the world, even within regions with networks that have been compromised.

DoD is developing 5G supply chain risk management strategies, guidelines, and procedures, and is working with industry, through standards bodies, to promulgate best practices. As an example, DoD is working closely with telecommunications industry leaders to develop an industry standard for 5G supply chain assurance via the Alliance for Telecommunications Industry Solutions (ATIS) standards development organization. This effort, among several others, endeavors to leverage existing acquisition and cybersecurity controls and processes to achieve U.S. national and economic security objectives.

In addition to Executive Order 13873, Section 889 of the FY 2019 National Defense Authorization Act prohibits federal procurement of certain Chinese telecommunications equipment and services. NDAA Section 889 prohibitions apply not only to federal procurement of items or services, but also to contracts with entities that use them, regardless of whether that usage is in performance of work under a federal contract. DoD implementation of Section 889 will enhance 5G supply chain security.

Further, DoD is a member of the newly established Federal Acquisition Security Council (FASC), whose purpose is to identify and recommend supply chain risk mitigation strategies that support a comprehensive and consistent approach across the whole of government. FASC efforts will directly apply to mitigating 5G supply chain risk.

GLOBAL OPERATIONS

DoD operates globally and will require the ability to securely use private, hybrid, and public 5G networks. DoD will work with industry, academia, standards setting bodies, and government research labs to develop and deploy techniques and technologies across DoD devices and infrastructure that ensure protected and resilient utilization of 5G networks globally, even in denied, degraded, intermittent, and limited environments.

DoD's "operate through" concept emphasizes the ability to operate on 5G infrastructure throughout the world. In many scenarios, DoD has permission to operate on another nation's 5G network through typical commercial relationships. However, DoD must assume that elements within the network environment are motivated to actively disrupt DoD's use of the 5G network infrastructure, and DoD must have a means to counteract this.

Permission to operate on another nation's 5G network entails some level of service level agreements that may include anticipated ranges on number of devices, bandwidth, latency, and reliability. As with any organization, one must anticipate any service level agreements offered within contested infrastructure may not be met. The DoD 5G "operate through" approach will use 5G technologies such as end-to-end network slicing and adaptive techniques such as dynamic spectrum utilization to enable DoD to achieve the capability necessary to accomplish the mission, regardless of whether the promised service level agreement is met by the 5G network.

In many scenarios, while DoD may have permission to operate on a 5G network, the underlying equipment may be capable of detecting and disrupting DoD communications. This could take the form of equipment exfiltrating data without the expressed knowledge of the network operator, the equipment appearing to fail in ways that are particularly disruptive to the DoD traffic, and potentially sending incorrect control messages that disruptive DoD's use of the network. Further, these non-DoD networks could be the subject of intentional electronic jamming at radio level and intentional configurations by network operational teams who may be opposed to the DoD mission. The complexity and diversity of 5G networks offer a wide range of potentially disruptive options to an adversary. However, this diversity in operational techniques also provides DoD with a number communication paths that can be used to ensure mission capabilities remain adequate despite efforts to disrupt DoD's use of the network.

SECURITY ASSESSMENTS

DoD will conduct security assessments to discover, assess, and mitigate 5G vulnerabilities. These actions include identifying vulnerabilities during development, deployment, and sustainment of 5G-enabled networks, platforms, and systems.

A risk analysis should be conducted for each 5G-enabled network, platform, or system to identify, assess and manage risk to DoD operations that use 5G. For example, three signaling networks must be assessed and managed: SS7,[5] DIAMETER,[6] and HTTP.[7] SS7 and DIAMETER have been notoriously insecure for years. The applications using 5G must be analyzed to determine if the known vulnerabilities within SS7 and DIAMETER cause high risk to the warfighter. Most of these types of vulnerabilities are related to the confidentiality of

[5] Q.700: Introduction to CCITT Signalling System No. 7, https://www.itu.int/rec/T-REC-Q.700.

[6] RFC 6733 – Diameter Base Protocol, https://tools.ietf.org/html/rfc6733.

[7] RFC 7540 - Hypertext Transfer Protocol Version 2 (HTTP/2), https://tools.ietf.org/html/rfc7540.

SMS and GPS coordinates, and roaming fraud. Some underlying vulnerabilities allow the use of interception of voice as well. Currently few mitigations are available.

Other security vulnerabilities associated with 5G must also be considered, including: vulnerabilities pertinent to the core network from network virtualization and slicing functions, the increased attack surface due to the higher quantity of unprotected/exposed small cells in denser network areas like cities (densification), risks introduced by moving computing closer to the cell sites (edge computing), threats due to massive numbers of IoT devices with limited security protections operating on 5G, and supply chain risks.

With the expected proliferation of 5G technologies within mobile applications, networks, platforms, and systems, it is imperative that DoD understands the potential risk of all such vulnerabilities being introduced into the 5G environment, as well as appropriate mitigation strategies. Many times, after the systems have been built and deployed, it becomes cost prohibitive to mitigate certain classes of vulnerabilities. Because of this, security testing and vulnerability detection must be implemented during development and throughout the system lifecycle.

To accomplish this, testing for vulnerabilities through simulated and emulated adversarial attacks must be conducted. This will allow DoD to assess the security strengths and weaknesses of the 5G environment and infrastructure. This vulnerability testing includes, but is not limited to, the associated networks, platforms, systems, and applications within the environment. Therefore, conducing a full-scale vulnerability assessment tends to be the most accurate methodology to discover previously unknown vulnerabilities.

For functionality, most 5G-enabled systems will use backend Application Programming Interfaces (APIs) as a part of the overall application. As APIs are often known trouble spots in web-based applications, 5G should be treated no differently. As such, these APIs need to be included in any security testing effort. Furthermore, to ensure communications themselves are properly secured, internal control testing as well as testing of the cryptographic controls are imperative. Without proper and securely implanted encryption throughout the entirety of the connection, the data's integrity and confidentiality could come into question.

After the 5G network, platform, or system is deployed, additional security testing should be conducted to ensure that local configurations have not introduced any new vulnerabilities. This process should continue through each patch, update and/or upgrade of the environment or infrastructure throughout its lifespan.

CYBERSECURITY AND ZERO-TRUST

The scale, complexity, and decentralized design of 5G architectures make it infeasible to depend upon perimeter security, which assumes that only trusted devices have been allowed inside the network. DoD will instead develop and validate a zero-trust model for 5G. The zero-trust approach will allow DoD to manage risk, while operating within untrusted network environments by utilizing encryption and fine-grained management of authorities and information access.

The zero-trust paradigm is ideally suited for the emerging 5G network infrastructure. A fundamental assumption of the DoD approach is that underlying equipment and software is not trusted and that some elements are intentionally disruptive to DoD communications. The 5G equipment and network operational practices will be under the control of telecommunications providers throughout the world, with a range of trustworthiness. Network equipment may be exfiltrating data without the expressed knowledge of the network operator. Network equipment or network operational practices may result in failures along communication paths used by DoD traffic, elements of the network and elements within transmission range may attempt to jam parts of the spectrum, and intentionally invalid control messages may be generated at any level of the 5G network.

Using the zero-trust approach, DoD is developing and demonstrating technologies for secure operations through insecure networks that incorporate new levels of vigilance and are built from untrusted and less-

than-trusted devices and systems. This will provide the availability, confidentiality, and integrity of data that is needed for DoD operations.

To address availability, DoD can leverage the complexity and diversity of 5G networks to provide robust communication and multi-path solutions. To overcome electronic jamming as well control plane based attacks against a particular path, DoD will demonstrate how various anti-jamming techniques, including dynamic spectrum utilization, require an adversary to continually evolve. These capabilities will be prototyped and evaluated at-scale within highly dynamic and contested RF environments.

To provide confidentiality, DoD is focusing on two fundamental techniques. First, it is essential to ensure data contents are appropriately protected with advanced adaptive encryption and key management technologies, and by properly enabling 5G confidentiality options. Second, adversary analysis of control messages and general communication patterns can be addressed through obfuscation techniques.

Integrity can be addressed in ways similar to confidentiality by using existing techniques for message authentication that are appropriately applied to the content of all messages. Integrity of control messages is more challenging, but can be overcome through the vast redundancy that 5G provides.

3. INFLUENCE 5G STANDARDS AND POLICIES:

5G represents a global technology; it is being developed, deployed, and regulated by numerous private and governmental organizations. The national and international standards to which 5G systems are designed will necessarily impact which companies and countries are best-positioned to provide those capabilities.

Because 5G is a global technology, and the DoD seeks to use 5G throughout its global operations, alignment with standards is critical to ensure that DoD can utilize technologies being developed and deployed by the 5G industry, leading to greater capabilities as well as cost savings. In most cases, DoD will be able to directly use 5G technologies. However, because of its mission, DoD also requires capabilities that go beyond those typically needed by industry. Therefore, DoD is working collaboratively with industry to influence standards to meet DoD's needs.

5G will also transform the way that DoD operates. Because of this, DoD is revisiting its spectrum management capabilities to align with the increasing use of the spectrum by industry, as well as the ways in which 5G can impact military operational planning and concepts of operations (CONOPS).

Although 5G is global, substantial technology and intellectual property development is done within the U.S., and much of this is relevant to national security. DoD will work with its interagency partners to ensure that U.S. technologies are protected.

STANDARDS SETTING BODIES

To promote high-quality, protected, and reliable 5G devices and applications, the U.S. must play a lead role in shaping information and communications technology standards. DoD will fully implement its Standards Engagement Plan and will actively participate in the 3rd Generation Partnership Project (3GPP) organization. It is vital that DoD and its interagency partners, including the Federal Communication Commission (FCC), National Institute of Standards and Technology (NIST), and National Telecommunications and Information Administration (NTIA), have specific and prioritized outcomes for this engagement, including strengthening U.S. influence in key standards setting organizations and promoting high-quality American 5G and beyond technologies.

DoD's approach to 5G standards engagement consists of establishing a dedicated Cross-Department Team (CDT) whose activities include sharing documentation, providing cross meeting representation, aligning voting, and identifying U.S. priorities. The 5G CDT is working cooperatively with industry and standards

organizations to become the 5G DoD standards focal point, and is working closely with other Federal agencies engaged in 5G standards (Figure 2).

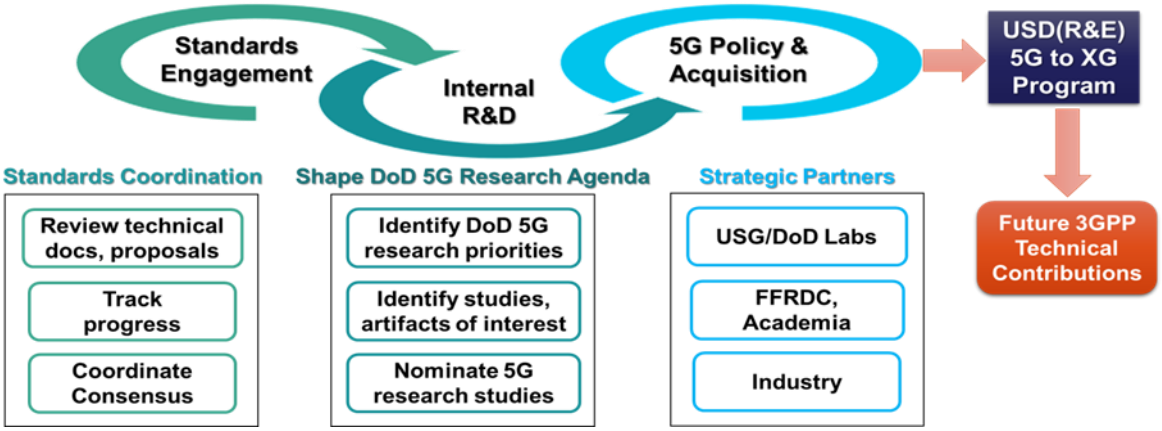

Figure 2 – DoD 5G Standards Overview

DoD Components have nominated Subject Matter Experts to the 5G CDT to participate in standards organizations in the areas of spectrum engineering, security, supply chain risk management, networking and services. 5G CDT members are expected to participate in multiple international meetings, and coordinate standards development with testing/technical evaluations from DoD 5G activities. The 5G CDT is developing technical contributions and papers (internally and collaboratively with vendor partners), and assessing vendor and operator marketplace positions and efforts. The 5G experiments will be used to evaluate the performance and improve the quality of these standards contributions.

DoD 5G CDT activities are divided into five technical areas. The five technical areas are in turn divided into sub-topics that focus on more specific projects (Figure 3). Standards project priorities for 5G CDT sub-teams for these topics are updated regularly to match the rapid pace of 5G technology evolution.

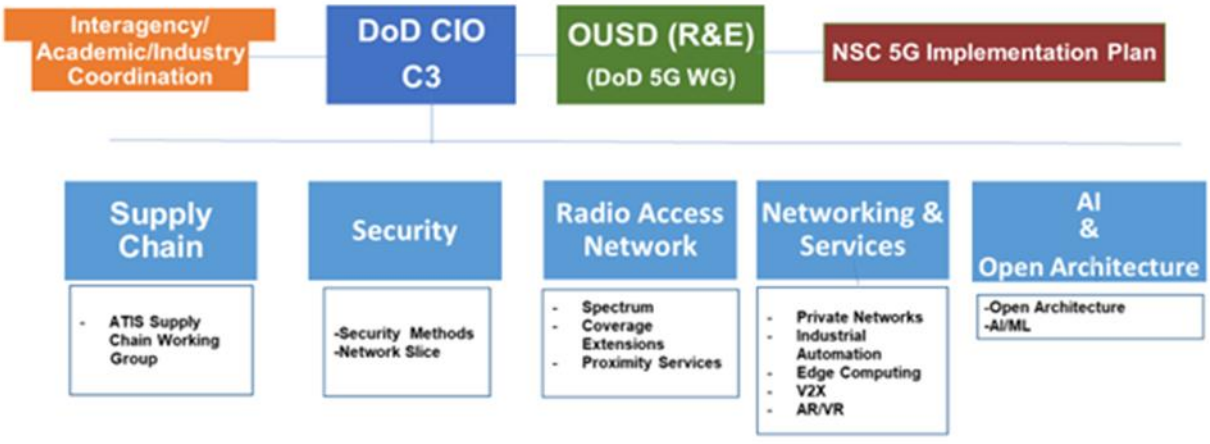

Figure 3 – DoD Standards Topics and Sub-teams

The 5G CDT sub-teams will engage, in collaboration with their aforementioned interagency, international, and industry partners, in specific standards setting bodies to shape 5G outcomes through both advocacy and submission of technical contributions. Standards setting bodies with which DoD has engaged include the Third Generation Partnership Project (3GPP), the Alliance for Telecommunications Industry Solutions (ATIS),

and the Institute for Electrical & Electronics Engineers (IEEE). Note that this list will be updated regularly to match the rapid pace of 5G technology evolution.

ADVANCED SPECTRUM MANAGEMENT

Traditional approaches to spectrum management – allotting slices of frequencies for single-purpose use – do not support the growing demand for spectrum for both civil and military innovation. As the 2018 Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future suggests, spectrum regulations and policies must keep pace with technological advances, growing spectrum demands, and operational realities. As the biggest user of Federal spectrum, DoD must continue to work closely with NTIA and the FCC to develop new policies for sharing spectrum, including dynamic spectrum sharing and bidirectional sharing of existing bands. 5G sharing decisions must be informed by technical feasibility and engineering analyses that ensure current and future DoD mission requirements can be satisfied. DoD seeks to demonstrate that this approach will provide both DoD and 5G network operators with greater spectrum access, capacity, and protection from interference. This approach will also pave the way for broader national adoption of spectrum sharing, which will help to spur 5G deployment, provide DoD with access to mission critical spectrum when needed, and improve resilience against coercive, illicit, and exploitative actions in the spectrum.

As noted in the Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future, the nation requires a balanced, forward-looking, flexible, and sustainable approach to spectrum management to help meet economic, national security, science, safety, and other Federal mission goals now and in the future. As the largest user of Federal spectrum, DoD must continue to work closely with NTIA and the FCC to develop new policies for utilizing spectrum in all bands. Technology advances can bring spectrum to market faster while protecting and enhancing flexible access for future military capabilities. At the same time, 5G spectrum decisions must be informed by technical feasibility and engineering analyses that ensure current and future DoD mission requirements can be satisfied. DoD seeks to demonstrate that this approach will provide both DoD and 5G network operators with greater spectrum access, capacity, and protection from interference. This approach will also foster U.S. leadership and adoption of spectrum technologies, speed 5G deployments, expand spectrum access for all users, and improve resilience against adversarial actions in the spectrum. To implement this approach, DoD will:

- Collaborate and integrate with the national regulators to develop a modernized national spectrum management IT architecture and associated analysis tools to expand spectrum access for all users.
- Advocate with Congress, the Administration, and the national regulators for regulatory and policy changes to support the development and implementation of innovative spectrum technologies and methodologies.
- Advance agile spectrum operations through allied partnerships with an emphasis on modernized electromagnetic battle management tools for command and control.
- Engage in partnerships with industry to mature innovative spectrum technologies and methodologies between DoD equities and 5G and beyond commercial capabilities.

5G-ENABLED CONCEPTS OF OPERATIONS

The deployment of 5G capabilities will offer a host of opportunities to both reform DoD enterprise services and to create powerful new military advantages. DoD will develop new concepts of operation to ensure its forces will be the first to harness the transformational speed and connectivity of 5G. DoD will explore and develop 5G-enabled capabilities across the full range of its missions and will ensure that it can achieve its mission objectives in contested and congested spectrum environments. The Military Departments will strengthen military effectiveness by integrating advanced information networks into the way U.S. forces are organized, trained, and equipped.

Employing the cutting edge of technology to enhance the posture of and create advantage for the Joint Force is critical to DoD enterprise and military operations, at home and abroad. DoD will adapt 5G and next generation technologies to "operate through" contested and constrained spectrum and compromised

networks to ensure maximum readiness, lethality, and partnering among allies. Transformational innovations expected to be implemented across the Joint Force include wireless, ubiquitous connectivity across humans, machines, and the Internet of Things. DoD will be an early adopter of disruptive 5G capabilities such as:

- Enhanced Mobile Broadband (eMBB) – higher quality and rich content services provided to multiple users with full mobility;
- Ultra-reliability and Low Latency (dramatically reduced latency) – supporting delivery of critical communications assured by ultra-reliable and low latency networks; and
- Massive Machine-to-Machine Communications – massive scale automation delivered through widespread sensor networks and multiple connected devices; sensor data from the Internet of Things (IoT) is widely considered as a primary driver for 5G.

The use cases for 5G apply across multiple industry segments, several which are relevant in the Defense context. 5G has the potential to become the communication fabric that supports new efforts in cloud-based AI enhanced distributed sensing. For example, a Smart Port or Smart Flight Line might include sensors (Internet of Things), edge computing, mobile/tablet handsets, augmented reality devices for maintenance, and automated vehicles (machine-to-machine communications). Although these are not new technologies introduced by 5G, it is the enablement at, or closer to, the customer edge that 5G heralds.

However, 5G also brings new dynamics and consequently threats to security and risk assessments. Beyond simply providing access to the mobile Internet for the foreseeable future, 5G networks will eventually supplant critical infrastructure communications and revolutionize several verticals such as transportation, logistics, and healthcare. Future 5G networks will be software-intensive, cloud-native, and increasingly managed by artificial intelligence (AI) algorithms. In order to ensure that the DoD can benefit from the technology while also reducing risk, any DoD 5G implementation must rest on a continuing commitment to understand and manage the expanding threat landscape.

TECHNOLOGY CONTROL MEASURES

DoD must also support whole-of-government efforts to protect 5G-enabling technologies from potential U.S. adversaries. This includes reviewing foreign investments in U.S. companies, updating and reviewing export controls, and other measures – while not compromising DoD's ability to acquire next-generation technologies. The Department must balance protecting sensitive information against the need for U.S. companies to collaborate and access international markets. These measures must be reviewed and updated regularly to match the rapid pace of technology evolution.

DoD is pursuing multiple methods for protecting 5G technologies. One key tool for protecting 5G-enabling technologies from adversarial capital is DoD's participation in the Committee on Foreign Investment in the United States (CFIUS). Through that mechanism, DoD can protect these technologies by reviewing and investigating, and when appropriate, prohibiting and suspending adversarial investment into relevant U.S. companies.

Additionally, through the DoD Foreign Investment Review (FIR) office's international and domestic outreach programs, DoD can share information on attempts by adversarial capital to undermine 5G-enabling technologies in foreign venues, especially those with a nexus to U.S. companies, and alert our allies and partners with regard to export control risk exposure.

FIR can also apply its analytical capability and collaboration with interagency partners to identify and mitigate adversarial capital investments not otherwise notified in CFIUS filings and to characterize market trends that could expose U.S. companies to threats from adversarial capital.

4. ENGAGE PARTNERS:

DoD must engage with interagency, international, and industry partners proactively to shape 5G outcomes. This requires positive, prioritized, and coordinated dialogue in support of our shared interests with each of these communities.

5G is an ecosystem spanning the globe, driven by industry, and operating within the guardrails of government. To advance DoD's goals in 5G, coordinated engagement with international allies and partners, industry, and the whole of government, and Congress will be crucial.

INTERNATIONAL ALLIES AND PARTNERS

DoD must collaborate closely with the State Department to utilize upcoming bilateral and multilateral dialogues to discuss 5G concerns with international partners. DoD must convey to allies and partners the risks to their national security equities — mobilization, interoperability, information sharing, operations, and resilience against coercion — to quickly address them before mitigations become far costlier. The matter is urgent, as many nations are already auctioning 5G spectrum and making long-term investments in 5G infrastructure. It is important that the United States promotes a shared understanding of the importance of 5G protection and the serious threat posed by unauthorized foreign access. The Prague Proposals on 5G security and the National Strategy to Secure 5G provide a helpful basis for framing this issue, specifically noting that "the overall risk of influence on a supplier by a third country should be taken into account".

The decisions made by our allies and partners about 5G deployment often involve senior government and industry leaders who may not view telecommunications infrastructure as a national security issue. DoD must ensure that foreign counterparts understand the risk 5G threats and vulnerabilities pose to interoperability and industrial security so they can accurately communicate the message across their governments. This requires DoD to provide a clear national security-based rationale concerning the risk of 5G vendors beholden to foreign governments.

Some states continue to seek to undermine fair and open international competition for 5G equipment and services via diplomatic pressure, misleading reporting, market manipulations, state-backed financing, and/or other aggressive interventions. The United States is confronting such tactics directly and ensuring that our allies and partners are aware of ties between foreign suppliers and their governments' security organizations. DoD will support these national-level efforts by collaborating with the global community to identify 5G security vulnerabilities and share relevant threat intelligence with DoD counterparts.

In order to influence significant upcoming decisions, DoD must develop clear, prioritized outcomes for international engagement and ensure DoD military, political, and industry outreach is aligned in support of those outcomes. This will include positive messaging about opportunities to collaborate with the United States on 5G research, standards, and deployment.

To implement this international engagement strategy, DoD is leveraging its ongoing engagements with allies and partners, including key leader engagements, to message them on the risks of allowing untrusted vendors onto their networks, while also identifying opportunities to counterbalance PRC technology proposals with U.S. or allied substitutes.

DoD is ensuring that key points from the DoD 5G Strategy are incorporated into bilateral and multilateral defense engagement talks under international outreach efforts. DoD also continues to refine talking points and messaging strategies to address country-specific concerns and build upon successful messaging efforts.

Further, DoD is prioritizing engagement with and support to allies and partners to develop 5G alternatives among countries that share our values and interests.

INDUSTRY ENGAGEMENT

DoD will continue to engage in open and transparent dialogue with our global industry partners, including 5G microelectronics manufacturers, telecommunications companies, and application developers. A healthy and robust National Security Innovation Base is vital to providing the United States with access to low-risk sources of components for the defense supply chain. DoD engagement with industry will continue to inform the U.S. approach to 5G standards, research priorities, and international collaboration. Only industry is able to deliver the 5G capabilities needed by DoD.

DoD's relationship with industry will be integral to all aspects of the implementation of the DoD 5G strategy. DoD will continue to engage in open and transparent dialogue with our global industry partners, including 5G microelectronics manufacturers, telecommunications companies, and application developers. A healthy and robust National Security Innovation Base is vital to providing the United States with access to low-risk sources of components for the defense supply chain. DoD engagement with industry will continue to inform the U.S. approach to 5G standards, research priorities, and international collaboration. Only industry is able to deliver the 5G capabilities needed by DoD.

A major purpose of the DoD 5G prototyping and experimentation efforts is to promote the innovation and success of U.S. industry. Each of the testbeds will incorporate solutions from both large and small U.S. companies. These companies will be developing solutions that will support DoD as well as their own customer base. The 5G ecosystem goes far beyond the basic network infrastructure. Relevant companies include those providing products and services such as devices, data centers, telecommunications transport, security, drones, autonomous vehicles, robotics, manufacturing equipment, healthcare equipment, augmented reality/virtual reality (AR/VR), and mobile device applications. As much as possible, DoD will deploy commercially available products and services to take advantage of scale and market innovations. The DoD 5G testbeds will serve as an excellent reference for U.S. companies to promote their solutions into the market.

DoD will also promote cooperation between the defense and telecommunications industries. This is already taking place through the National Defense Industry Association's efforts to bring defense and telecommunications companies together to support 5G spectrum operations and regulations optimizations. Additionally, DoD will explore opportunities for enhancing collaboration between U.S. and international partner industry entities on topics such as 5G research, development, testing, and evaluation.

CONGRESSIONAL ENGAGEMENT

Many aspects of national 5G development and deployment are shaped by legislation. U.S. companies require adequate access to capital to deploy 5G infrastructure, along with fair, competitive access to global markets. DoD will work with interagency partners to identify and recommend specific legislative proposals to strengthen 5G standards and security, incentivize deployment, and offset distortions to the open market.

Congressional support for DoD 5G efforts, including DoD's 5G prototyping and experimentation program, has been critical to accelerating DoD's adoption of 5G technologies, its efforts to secure 5G systems, and its plans to promote technology development for both 5G and future generations of wireless technology.

DoD will continue to actively engage with Congress to strengthen national and DoD 5G capabilities. In particular, the ongoing experimentation activities will help identify specific issues needing legislative consideration, such as ways to eliminate barriers to rapid network deployment, or to incentivize 5G security.

CONCLUSION

This document has described how the DoD will approach the implementation of the DoD 5G Strategy by promoting technology development, assessing, mitigating, and operating through 5G vulnerabilities, influencing 5G standards and policies, and engaging partners. 5G and future "next G" technologies are critical to the U.S. networked way of war. The DoD 5G Strategy and this implementation plan will help ensure that the U.S. military, the American public, and our allies and partners have access to the best 5G systems, services, and applications in the world.