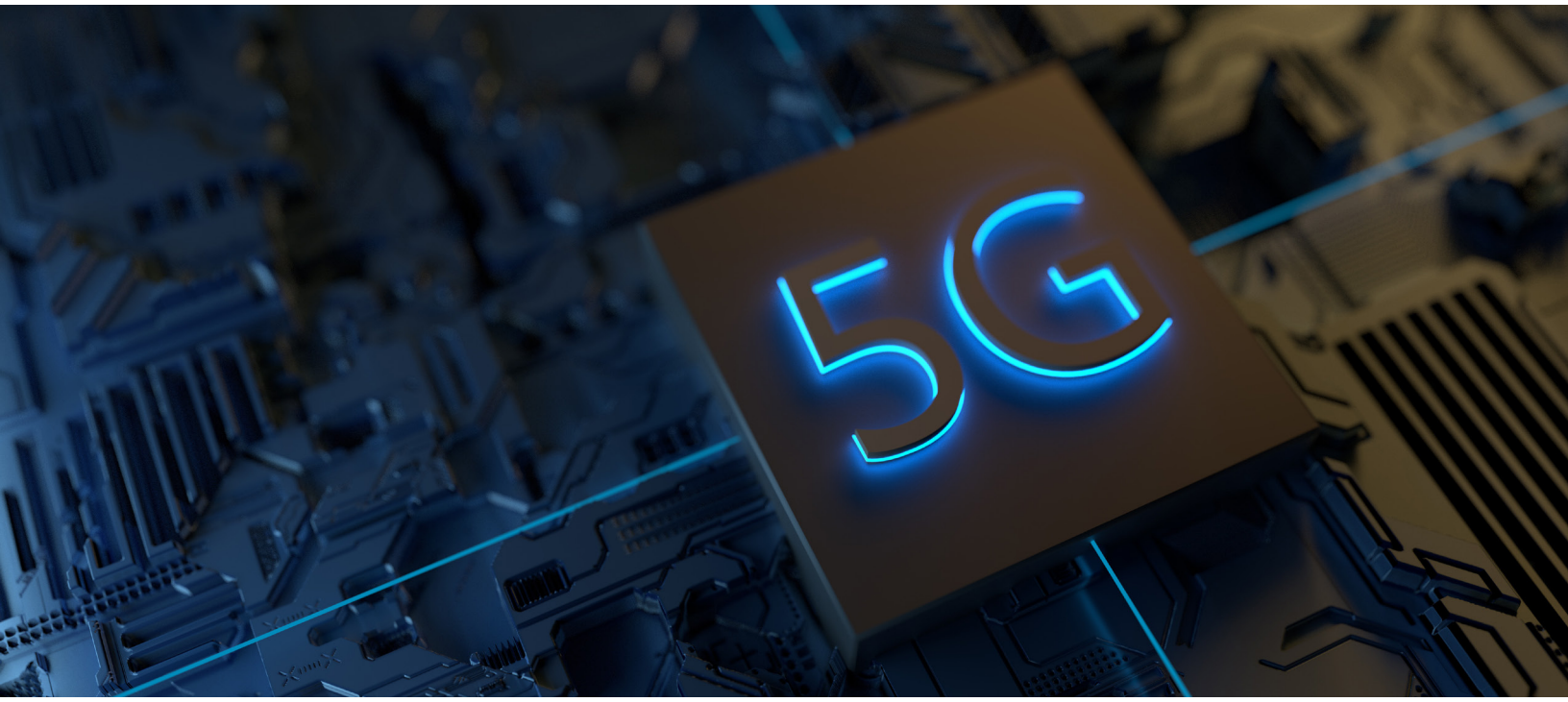
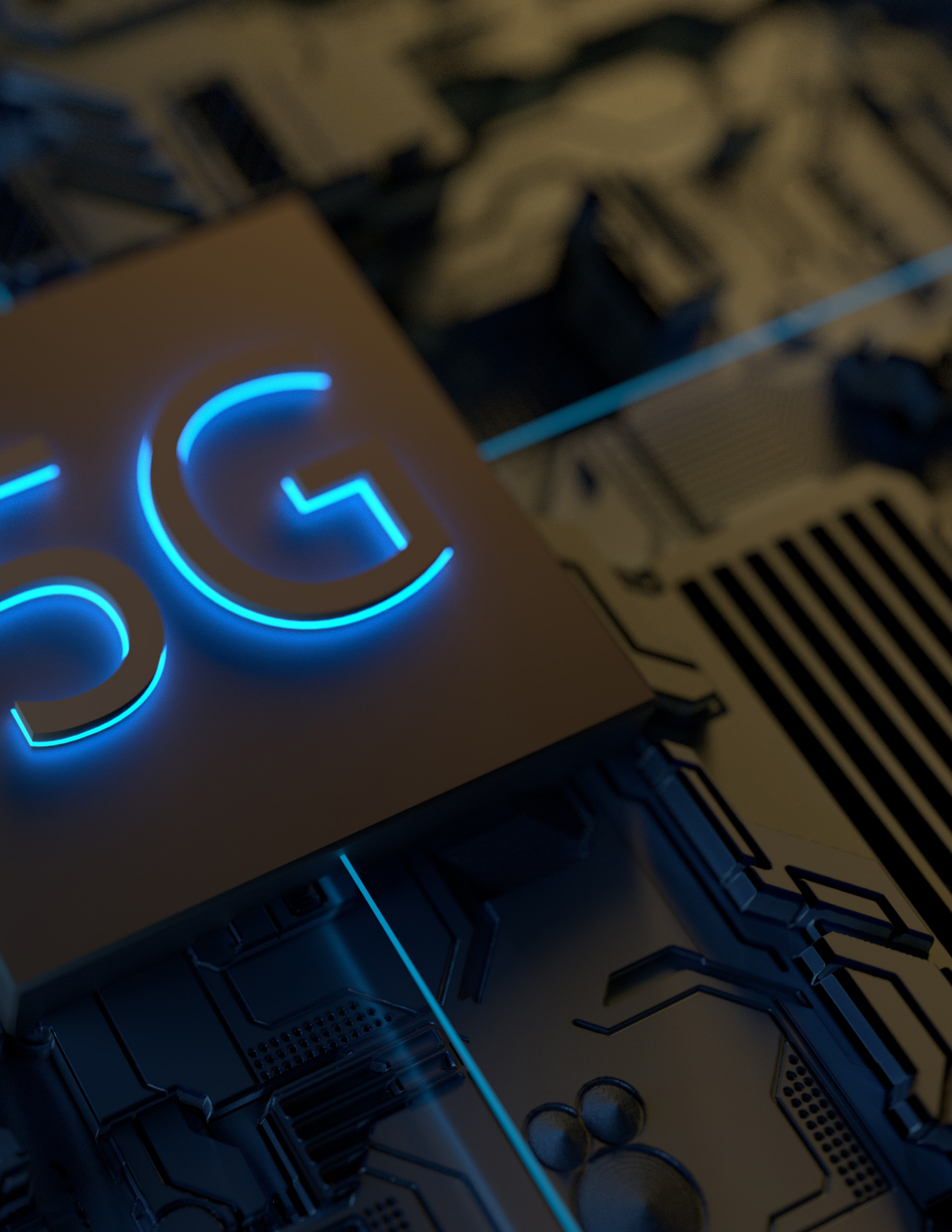
Homeland Security



SECURITY IMPLICATIONS OF 5G TECHNOLOGY:

Overview and Recommendations

2021
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM


5G

EXECUTIVE SUMMARY

The fifth-generation (5G) of wireless technology represents the next evolution of mobile communications networks, introducing a wealth of new connections, capabilities, and services. From autonomous vehicles to telesurgery, 5G will revolutionize the way the world communicates and shares information. However, the adoption and deployment of 5G introduces a range of vulnerabilities that could increase risk for the United States and its allies. Given 5G's impact, the stakes for protecting these networks could not be higher.

The Public-Private Analytic Exchange Program (AEP), sponsored by the Department of Homeland Security's Office of Intelligence and Analysis (DHS/I&A), on behalf of the Office of the Director of National Intelligence (ODNI), facilitates collaborative partnerships between members of the private sector and teams of experienced U.S government analysts to form several subcommittees. This partnership helps enable the US Government and private sector partners to gain a greater understanding of how their complementary roles can lead to analytical products that enhance their unique missions.

The 2021 Public-Private AEP Privacy and Security Implications of 5G Technology Team examined new privacy and security implications associated with 5G technology, which will radically improve the bandwidth, capacity, and reliability of mobile broadband. Comprised of individuals from national security/intelligence entities, industry, defense contractors, and critical infrastructure sectors, the team identified three primary 5G focus areas, 1) Standards; 2) Cybersecurity and Supply Chain Security; and 3) Vendor Diversity and Economic Competition. Within each of these focus areas, the Team documented existing key areas of work, which includes initiatives and resources developed by various federal departments and agencies, and analyzed them to identify recommendations for future collaboration. These recommendations can be used to support the development of future 5G work-streams, inform funding, and/or influence policy decisions.

DISCLAIMER STATEMENT: *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.*

TEAM INTRODUCTIONS

MEMBER	COMPANY
Chair: Christopher Alexander	Cybersecurity and Infrastructure Security Agency (CISA), National Risk Management Center (NRMC)
Co-Chair: Serena Reynolds	CISA, NRMC
Technical Support: Andrew Holcomb	CISA, NRMC
Technical Support: Aleida Baumgartner	CISA, NRMC
Team Member: Alexandra S	Federal Bureau of Investigation
Team Member: Anna Sarnek	RSA Security LLC
Team Member: Devon Fitzgerald	Thomson Teuters Special Services
Team Member: Honoré Nyuyse	DHS Science and Technology Directorate (S&T)
Team Member: Richard Schumaker	The University of North Carolina at Greensboro
Team Member: Melanie Tiano	CTIA - The Wireless Association
Team Member: Robert Mayer	USTelecom
Team Member: Courtney Lang	Information Technology Industry Council (ITI)
Team Member: Drew Morin	T-Mobile
Team Member: Rudy Brioche	Comcast

CONTENTS

Introduction 01

Focus Area 1: Standards 02

Focus Area 2: Cybersecurity and Supply Chain Security 09

Focus Area 3: Vendor Diversity and Economic Competition 14

Conclusion 16

INTRODUCTION

5G is poised to be the most secure generation of wireless networks yet, and the evolution to this next generation presents opportunities to enhance security and create a better user experience. Monitoring and mitigating cyber threats will continue to be critical, including when it comes to supply chains, deployment, network security, and competition and choice. In particular, cybersecurity stakeholders are focused on mitigating the following risks in the U.S. as networks migrate to 5G: risk of dominance by untrusted entities in the global supply chain, lack of broader vendor diversity and interoperability efforts, increased penetration of 5G infrastructure, integration within existing legacy networks, and the risk of untrusted custom code for information and communications technology (ICT) components.

In light of the security opportunities and challenges associated with 5G, our team was challenged to identify which area of emphasis would provide the best value for the time and effort of participants. Our commercial partners, represented by the Communications Sector Coordinating Council (CSCC) and the Information Technology Sector Coordinating Council (ITSCC), readily worked with us on identifying areas of opportunity, and the enhanced partnership recognized the value in mapping out the many 5G security efforts currently ongoing within the U.S. and creating recommendations on future efforts.

FOCUS AREA 1: STANDARDS

KEY AREAS OF WORK

Department of Homeland Security (DHS)

DHS is the lead federal agency for cybersecurity and is helping shape the rollout of this emerging critical infrastructure through strategic risk mitigation initiatives that stem from the *National Strategy to Secure 5G*. DHS is working with interagency, industry, and international partners to ensure that there are policy, legal, security, and safety frameworks are in place to mitigate significant 5G risks. Some of the recent engagements and activities on 5G are as follows:

- As a risk advisor through the National Risk Management Center (NRMC), DHS through the Cybersecurity Infrastructure Security and Resiliency Agency (CISA) is leading risk mitigation efforts by working with government and industry partners to ensure the security and resiliency of 5G technology and infrastructure.[1]

- During the 2nd quarter of FY21, DHS CISA, in coordination with the National Security Agency, and the Office of the Director of National Intelligence, as part of the Enduring Security Framework (ESF)—a cross-sector, public-private working group—released the *Potential Threat Vectors to 5G Infrastructure* paper.[2]

[1](U) DHS Cybersecurity Infrastructure Security and Resiliency Agency (CISA) | 2020 | CISA 5G Strategy | 5G Security and Resiliency
[2](U) DHS CISA | 10th, May 2020 | Potential Threat Vectors to 5G Infrastructure

- Testbeds and Pilots: In the 4th quarter of FY20, CISA announced during its Annual Cybersecurity Summit that it is launching a technical assistance pilot program to address state and local 5G security and deployment. The pilot is launching with the Federal Bureau of Investigation (FBI), Department of State (DoS), Department of Defense (DoD), the Federal Communications Commission (FCC), and the National Telecommunications and Information Administration (NTIA). Likewise, DHS CISA later released the *Framework to Conduct 5G Testing* by the Federal Mobility Group (FMG).[3]

- DHS continues collaboration with the National Institute of Standards and Technology (NIST) and FCC and participates in the development of 5G technical specifications and standards through forums such as the International Telecommunication Union (ITU), a specialized agency of the United Nations that coordinates the standardization of international communications networks, and the Third Generation Partnership Project (3GPP), the international organization responsible for the development of technical specifications.[4]

- Within the research and development (R&D) domain DHS has partnered with the National Science Foundation (NSF),NIST, NTIA, the DoD, and the Department of Energy (DoE) to fund and conduct R&D for 5G and future mobile wireless technologies. These agencies are coordinating R&D priorities and investments through the Networking and Information Technology Research and Development (NITRD) program, a multiagency program that operates under the aegis of the White House Office of Science and Technology Policy.

The United States Department of Defense (DoD)

The DoD is at the forefront of cutting edge 5G testing and experimentation intended to be transformative across the Nation's warfighting capabilities. In FY20, DoD announced $600 million for 5G testbeds across five U.S. military sites, representing the largest full-scale 5G tests for dual-use applications in the world. Through this effort, the Department partners with industry to test 5G operations such as augmented and virtual reality training, smart warehousing, and distributed command and control.[5, 6, 7] In 2021, the Department will be announcing a second tranche of awards at seven more test sites. Similar DoD 5G initiatives include:

- DoD Chief Information Officer in partnership with Office of the Under Secretary of Defense for Research and Engineering (OUSD R&E) is putting together a team

[3](U) DHS CISA | 2020 | CISA 5G Strategy
[4](U) Federal Mobility Group | November 2020 | 5G Framework To Conduct 5G Testing
[5](U) Department of Defense | 9th, October 2020 | DoD Kicks Off World's Largest Dual-Use 5G Testing Effort
[6](U) Federal Mobility Group | November 2020 | 5G Framework To Conduct 5G Testing
[7](U) Department of Defense | 3rd April 2019 | The 5G Ecosystem: Risks & Opportunities for DoD

to begin tracking current activities in international standards organizations to identify areas of interest or concern related to missions.

- In September 2020 DoD sought stakeholder comments through its Dynamic Spectrum Sharing request for information (RFI). The RFI is intended to seek information on innovative solutions and alternative approaches to enable dynamic spectrum sharing within the Department's currently allocated spectrum with the goal of accelerating spectrum sharing decisions and 5G deployment.[8]

- In April 2021, OUSD R&E, in coordination with the National Security Council (NSC), plan to carry out a coordinated R&D Program designed to accelerate enhancing mission effectiveness, streamlining and upgrading communications infrastructure, improving efficient spectrum utilization, and advancing microelectronics to enable protected and resilient networks.[9]

General Services Administration (GSA)

GSA has acquisition initiatives for mobility products and services, such as wireless carrier services, mobile devices, mobile hardware and infrastructure, and the Internet of Things (IoT). Information technology operates the Technology Modernization Fund's (TMF) Program Management Office (PMO). The TMF PMO works with agencies to build technology modernization business cases and aids in all phases of the acquisition lifecycle. GSA is also overseeing the Federal Strategic Sourcing Initiative for Wireless. By executive order, GSA is coordinating all wireless telecommunications installations on federal property and has consolidated a number of forms, leases, and contracts to help speed the deployment of wireless infrastructure.[10] Similarly, GSA hosted a 5G symposium to bring together industry and government to identify use cases and insights around 5G technology, standards, security, and acquisition.[11]

Federal Communications Commission (FCC)

The FCC is working on 5G deployment and security. The FCC's plan to Facilitate America's Superiority in 5G Technology is working to push more spectrum into the marketplace, update infrastructure policy, and modernize outdated regulations.[12] In September 2019, the FCC released a Public Notice and press release establishing two innovation zones to empower Advanced Wireless Technology and 5G-Ready network experimentation. The test beds extend the geographic areas in which already-licensed experimental program licensees can conduct tests.[13] Similarly, the FCC's Technical Advisory Council (TAC) has

[8](U) Department of Defense | 18th September 2020 | Defense Spectrum Sharing Request for Information | SAM.gov
[9](U) Department of Defense | 14th April 2021 | Intent to Announce Request for Prototype Proposals (RPP) under the Spectrum Forward Other Transaction Agreement | SAM.gov
[10](U) Federal Mobility Group | November 2020 | 5G Framework To Conduct 5G Testing
[11](U) General Services Administration | 3rd, September 2019 | GSA 5G Government Symposium
[12](U) Federal Mobility Group | November 2020 | 5G Framework To Conduct 5G Testing
[13](U) Federal Communication Commission | 16th September 2019 | FCC Establishes First Two Innovation Zones

worked on multiple 5G efforts, including at a recent December 2020 meeting where the TAC unveiled recommendations from four working groups, chartered to look at: Artificial Intelligence (AI), the Future of Unlicensed Spectrum, 5G Radio Access Network (RAN), and 5G IoT.[14]

National Institute of Standards and Technology (NIST)

NIST, is leading the Advanced Communications Program, which is focused on three topics: federal engagement in 5G standards development, advanced communications R&D and testing enhanced spectrum, and efforts to secure advanced communications.[15] NIST's Resilient and Intelligent Next-Generation Systems (RINGS) program brings together federal agency and industry partners to accelerate research on wireless and mobile communication networks and associated computing systems and large-scale services. The program will seek to advance the underlying technologies to guarantee worldwide availability, security and reliability of next-generation (NextG) systems.[16] NIST also sponsors the NextG Channel Model Alliance, formerly known as the 5G millimeter-Wave (mmWave) Channel Model Alliance, which is a research consortium aimed at advancing breakthrough through measurement, calibration, and channel modeling approaches, and technologies used for mmWave and submillimeter-wave frequencies.[17]

NIST has also developed several resources to further 5G measurement and analysis. On March 18, 2020, NIST announced the development of a 5G Spectrum Sharing Test Bed, an adaptable network that can measure how well 5G and older systems, such as Wi-Fi, GPS and military radar, can operate without interfering with each other on increasingly crowded airwaves (i.e. spectrum sharing). NIST is also in the process of upgrading a test bed named the NIST Broadband Interoperability Test Bed with the end goal of including a suite of four new shielded rooms to enable testing across multiple chambers.[18] On August 10, 2020, NIST announced another resource nicknamed SAMURAI, or Synthetic Aperture Measurements of Uncertainty in Angle of Incidence, which is the first portable system to provide 5G wireless measurements with accuracy that can be traced to fundamental physical standards. While many existing tools can measure some aspects of 5G device and channel performance, these measurements are more of a general overview of a channel, whereas SAMURAI provides more precise details. This tool can be used to address intelligence gaps surrounding 5G's use of active antennas, such as what is the outcome when high data rates are transmitted across multiple channels at once.[19]

[14](U) Federal Communication Commission | 18th September 2019 | Office of Engineering And Technology Announces First Innovation Zones For Program Experimental Licenses
[15](U) National Institute of Standards and Technology | 2021 | Advanced Communications | Source is the NIST official website.
[16](U) National Institute of Standards and Technology | 27 April 2021 | NIST Joins NSF-Led Partnership to Support Next-Generation Communicatios
[17](U) National Institute of Standards and Technology | 2021 | NextG Channel Model Alliance | Source is the NextG Channel Model Alliance official homepage.
[18](U) National Institute of Standards and Technology | 18 March 2020 | NIST Helps Build Accurate Measurement Infrastructure for 5G Communications | Source is the NIST official website.
[19](U) National Institute of Standards and Technology | 10 August 2020 | NIST's SAMURAI Measures 5G Communications Channels Precisely | Source is the NIST official website.

National Science Foundation (NSF)

The NSF, an independent agency of the U.S. government that supports research in non-medical fields of science and engineering, has engaged in advanced wireless research, 5G dataset research, and spectrum innovation. NSF is advancing wireless research through partnerships and initiatives, experimentation on testbeds, workforce development amongst academic, industry and community leaders, and participation in the NITRD Wireless Spectrum R&D Interagency Working Group and Advanced Wireless Test Platforms team.[20]

NSF is also leading a Spectrum Innovation Initiative to address issues arising from the increasing demand for the use of electromagnetic spectrum. The goal of the initiative is to promote dynamic and agile spectrum use, while ensuring security. NSF intends to further this initiative through research, infrastructure development, collaboration, public outreach, education and workforce development.[21] In February 2021, the FCC and NTIA announced its support and agreement with the NSF Spectrum Innovation Initiative.[22]

In March 2021, NSF demonstrated an intention to advance the development of next-generation, high-performance networks and computer systems through a request for information (RFI). The NSF RFI specifically requested participants provide representative datasets such as spectrum data, physical layer data, network and Internet measurement data, workload data, power/performance data, and other systems data. NSF also stated its interest in assessing where research progress is slowed due to the lack of datasets that may either already exist or can be generated using existing infrastructure and future investments.[23]

National Telecommunications Industry Association (NTIA) and DoD

NTIA, which falls within the Department of Commerce and advises the Office of the President on telecommunications policy, and the DoD have partnered on select projects to both develop spectrum-sharing capabilities and further develop the open 5G stack ecosystem. In December 2020, the Office of Spectrum Management of the NTIA established an Incumbent Informing Capability (IIC) team to collaborate with the DoD. The goal of this team was to develop an innovative spectrum-sharing concept that would enable federal spectrum to be shared in some instances where agencies use it only episodically or in limited areas. The IIC concept is a time and location-sensitive spectrum sharing methodology that would enable DoD and other federal agencies that are using

[20](U) National Science Foundation | 27 April 2021 | Advanced Wireless Research at NSF.
[21](U) National Science Foundation | July 2021 | NSF's Spectrum Innovation Initiative.
[22](U) Federal Communications Commission | 1 February 2021 | FCC, NTIA, and NSF Sign Agreement to Support NSF Spectrum Innovation Initiative | Source was an unofficial announcement of Commission action.
[23](U) National Science Foundation | 15 March 2021 | Dear Colleague Letter: Request for Information on the specific needs for datasets to conduct research on computer and network systems | The NFI RFI invites individuals and groups of individuals to provide input via an online submission form for a particular need.

spectrum to submit information securely about when and where they would be using certain frequencies. As of February 2021, the IIC team efforts are ongoing.

In January 2021, the NTIA published a Notice of Inquiry (NOI) seeking comment on the "creation of a 5G Challenge that would accelerate the development of the open 5G stack ecosystem in support of Department of Defense missions." NTIA published the NOI under sponsorship and in collaboration with the DoD 5G initiative, which was established in 2019 with the goal to advance U.S. and partner capabilities to fully leverage 5G technologies for military networking needs.[24] At least 51 software development and telecommunications organizations provided responses to the NOI and DoD efforts under this plan remain ongoing.[25]

The White House

The White House has provided messaging prioritizing 5G security via the Office of Science and Technology Policy (OSTP). OSTP advises the Executive Office of the President on, amongst other things, technological aspects of the economy, national security, homeland security, and foreign relations with respect to major Federal policies, plans, and programs. In May 2019, OSTP published two reports titled "Research and Development Priorities for American Leadership in Wireless Communications" and "Emerging Technologies and Their Expected Impact on Non-Federal Spectrum Demand." Both OSTP reports acted as a response to an October 2018 Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future that recommended prioritizing research and design to advance radio frequency spectrum access.[26]

The first report focusing on national spectrum research and development (R&D) priorities contained recommendations to improve the economic impact of electromagnetic spectrum for an increasingly wide range of communications, networking, location, and other applications while protecting national security and public safety.[27] The second report focused on new technologies expected to gain popularity with the advent of 5G and advised that the United States must employ new methods of spectrum use in order to achieve long-term success using 5G networks in a secure fashion.[28]

---

[24](U) National Telecommunications and Information Administration | 11 January 2021 | Federal Register, 5G Challenge Notice of Inquiry| Vol. 86, No. 6, p. 1949 | The Federal Register is the official daily journal of the federal government of the United States that contains government agency rules, proposed rules, and public notices.

[25](U) National Telecommunications and Information Administration | 16 February 2021 | Comments on 5G Challenge Notice of Inquiry|The Federal Register is the official daily journal of the federal government of the United States that contains government agency rules, proposed rules, and public notices.

[26](U) Administration of Donald J Trump | 25 October 2018 | Memorandum for the Heads of Executive Departments and Agencies | Section 2(c) | Presidential memorandum for heads of executive departments and agencies.

[27](U) Executive Office of the President | May 2019 | Research and Development Priorities for American Leadership in Wireless Communications | p.1 | OSTP report.

[28](U) Executive Office of the President | May 2019 | Emerging Technologies and Their Expected Impact on Non-Federal Spectrum Demand | p.13 | OSTP report.

RECOMMENDATIONS

- Develop a unified national strategy on promoting trusted, industry-led 5G and 6G telecommunications standards.
- Encourage increased industry presence on telecommunications standards bodies (e.g., 3rd Generation Partnership Project, International Telecommunication Union, and Institute of Electrical and Electronics Engineers) to influence the adoption of trusted standards that benefit the U.S. and its allies.
- Unify telecommunications standards efforts and collaboration across U.S. Departments and Agencies, in support of U.S. industry partners.
- Engage with international partners to promote trusted 5G and 6G industry-led standards.

FOCUS AREA 2: CYBERSECURITY AND SUPPLY CHAIN SECURITY

KEY AREAS OF WORK

Department of Commerce (DoC)

ICT Supply Chain Rule: On 1/19/2021, Commerce published its information and communications technology and services (ICTS) supply chain Interim Final Rule under Executive Order 13873: Securing the ICTS Supply Chain issued on 5/15/2019.

Foundational Technologies: On 8/27/2020, DoC's Bureau of Industry and Security (BIS) issued an advance notice of proposed rulemaking on Foundational Technologies. BIS will evaluate specific items, including items currently subject only to anti-terrorism controls on the Commerce Control List or those designated as Export Administration Regulations (EAR) 99.

Emerging Technologies: On 1/6/2020, BIS issued "emerging technology" interim rule to control artificial intelligence-based software specially designed to automate the analysis of geospatial imagery and point clouds.

DHS

Potential Threat Vectors to 5G Infrastructure: On 5/10/2021 CISA, in coordination with NSA and the Office of the Director of National Intelligence (ODNI), as part of the Enduring Security Framework (ESF), published the *Potential Threat Vectors to 5G Infrastructure*.

CISA 5G Strategy: The CISA 5G Strategy was released in August 2020. It was preceded by a CISA 5G infographic on network risk factor and Overview of Risks Introduced by 5G Adoption in the United States.

CISA Edge vs. Core Report: Edge vs. Core - An Increasingly Less Pronounced Distinction in 5G Networks released December 2020.

CISA Risks Introduced by 5G Adoption: Overview of Risks Introduced by 5G Adoption in the United States released in July 2019.

CISA Risks to Telecommunications Central Offices: CISA and the NRMC recently released an infographic relating to Risks to Critical Infrastructure: Telecommunications Central Offices.

DHS Science & Technology (S&T) Projects: 5G Introduces New Benefits, Cybersecurity Risks. DHS S&T also released a Broad Agency Announcement (BAA) Call for Secure and Resilient Mobile Network Infrastructure amended 2/27/2020.

- DHS announced 2 R&D awards in March 2021 and announced 7 awards in February 2021

ICT Supply Chain Risk Management Task Force: In response to requirements in EO 13873, the ICT SCRM Task Force, comprised of industry and government partners have worked to:

- Develop a standardized taxonomy of ICT elements (e.g., hardware, software, and services)
- Perform criticality assessments on these ICT elements with appropriate stakeholder input
- Assess the national security risks stemming from vulnerabilities in ICT hardware, software, and services including components enabling 5G communications

DHS-NSTAC Reports: The National Security Telecommunications Advisory Committee (NSTAC) has published numerous reports to the President related to 5G and communications security. Including, among others:

- NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the ICT Ecosystem;
- NSTAC Report to the President on Software-Defined Networking; and
- Most recently, at the 5/6/2021 NSTAC meeting, the group approved a NSTAC Report to the President on Communications Resiliency

NIST 5G Test Beds:

- Announced on 3/18/2020, "NIST is helping to build the crucial measurement infrastructure for emerging wireless systems by developing new measurement methods and analysis tools and by facilitating the sharing of 5G performance

data."

- On 8/10/2020, NIST announced that it also developed a "portable measurement system to support design and repeatable laboratory testing of fifth-generation (5G) wireless communications devices with unprecedented accuracy across a wide range of signal frequencies and scenario," called SAMURAI.
- NIST also supports studies at the National Broadband Interoperability Test Bed (NBIT).

NextG Channel Model Alliance: The NextG Channel Model Alliance (formerly operated as the 5G Millimeter-Wave (mmWave) Channel Model Alliance) is a NIST-sponsored international research consortium working to advance breakthrough measurement, calibration, and channel modeling approaches and technologies used for mmWave and submillimeter-wave frequencies

DOD

Darpa Projects: A BAA was issued in January 2020 related to Open, Programmable, Secure 5G (OPS-5G).

FCC

Equipment Authorization and Spectrum Auctions Proceeding: On 5/27, the FCC released a draft Notice of Proposed Rulemaking (NPRM) and Notice of Inquiry (NOI) proposing significant changes to the FCC's equipment authorization regime and spectrum auction certifications, intended to protect U.S. communications networks from equipment and services that pose an unacceptable risk to national security.

Supply Chain Security Proceeding: The FCC's Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs proceeding has been a multi-year effort with numerous notice and comment periods and recently established rules.

FCC CSRIC: The FCC's Communications Security, Reliability, and Interoperability Council (CSRIC) has produced multiple reports on communications and 5G security and resiliency, including, among others:

- CSRIC VII Report on Risk to 5G from Legacy Vulnerabilities and Best Practices for Mitigation;
- CSRIC VII Report on Risks Introduced by 3GPP Releases 15 and 16 5G Standards;
- CSRIC VII Report on Review and Recommendations on Optional 3GPP Standards for 5G Non Standalone Architecture; and
- CSRIC VII Report on Recommendations for Identifying Optional Security Features That Can Diminish the Effectiveness of 5G Security.

Federal Bureau of Investigation (FBI)

The FBI continues to investigate, identify, and share threat-based tradecraft, and support indictments of 5G-related vendors engaged in criminal activities such as intellectual property and trade secret theft and fraud. Information regarding these investigations can be found on the FBI's website or through Infragard, an FBI and private sector partnership focused on critical infrastructure protection. The FBI's Internet Governance Program Office maintains membership and public safety advocacy in 5G-related standards organizations such as 3GPP, ITU, and the Internet Corporation for Assigned Names and Numbers (ICANN). FBI participation is coordinated with both U.S. Government leads for the groups and private sector partners.

Government Accountability Office (GAO)

GAO Report: National Security: Additional Actions Needed to Ensure Effectiveness of 5G Strategy.

NIST

NIST Securing the 5G Supply Chain Workshop: NIST hosted a virtual workshop on May 18-19 on measurement-based approaches for authenticating 5G hardware. The findings will be summarized in a NIST Special Report tentatively planned for public release in 2021.

National Cybersecurity Center of Excellence (NCCoE) 5G Cybersecurity Project: NIST through NCCoE launched the Preparing a Secure Evolution to 5G project and practice guide. It is a proof-of-concept solution that will integrate commercial and open source products that use cybersecurity standards and recommended practices to showcase 5G's security.

NCCoE Trusted Cloud Project: NIST through NCCoE is working on publications on hardware-enabled security as part of the NCCoE Trusted Cloud project, such as Draft NISTIR 8320, Hardware-Enabled Security: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases.

White House/NTIA

National Strategy to Secure 5G: On March 23, 2020, the President signed into law the Secure 5G and Beyond Act of 2020 (S.893), which required the development of a strategy to ensure the security of next-generation wireless communications systems and infrastructure. [this may be best addressed in a separate, preliminary discussion] The National Strategy to Secure 5G, establishes four lines of effort:

- Facilitating domestic 5G rollout;
- Assessing cybersecurity risks to and core security principles of 5G capabilities and infrastructure;

- Addressing risks to US economic and national security development and deployment of 5G; and
- Promoting responsible global development of secure and reliable 5G infrastructure

National Strategy to Secure 5G Implementation Plan: NTIA issued a Request for Comments on the National Strategy to Secure 5G Implementation Plan in May 2020. NTIA received more than 80 industry and stakeholder comments in response to its Request for Comments.

Communications Supply Chain Risk Information Partnership: NTIA established the Communications Supply Chain Risk Information Partnership (C-SCRIP), to share supply chain security risk info with trusted communications providers and suppliers. C-SCRIP was called for in Secure and Trusted Communications Networks Act of 2019. The goal is to improve small and rural communications providers' and equipment suppliers' access to information about risks to key elements in their supply chain.

ODNI

Supply Chain Risk Management: Among other efforts, ODNI's National Counterintelligence and Security Center (NCSC) maintains a supply chain risk management website that addresses 5G and the ICT supply chain, with multiple cross-government resources.

RECOMMENDATIONS

- Coordinate federal efforts related to 5G security and supply chain to eliminate duplication and ensure consistency.

- Coordinate federal work in the United States on 5G security test beds, with a goal to reduce duplication and inefficiency and focus on harnessing private sector test bed work that can feature live or realistic networks.

- Share information about and consider partnering across borders on test bed efforts that are aligned with the US, with a priority given to private sector test beds that examine operationally relevant 5G use cases.

- Conduct after-action evaluations and cost benefit analyses of federal initiatives, such as C-SCRIP, to identify lessons learned and areas for improvement in government information sharing and activity.

- Solicit input from developers and operators of advanced communications networks about what they want from government as it relates to security, to better deploy scarce government resources.

FOCUS AREA 3: VENDOR DIVERSITY & ECONOMIC COMPETITION

KEY AREAS OF WORK

FCC

5G Future Plan: The FCC's America's 5G Future plan (formerly called the 5G FAST Plan) has 3 parts: (1) opening up more spectrum; (2) updating outdated infrastructure policy; and (3) streamlining and modernizing regulations.

Semiconductor Shortage Proceeding: On 5/11/2021, the FCC's Wireless Telecommunications Bureau released a Public Notice, seeking comment on the Impact of the Global Semiconductor Shortage on the U.S. Communications Sector.

Open RAN Proceeding: The FCC approved a Notice of Inquiry seeking comment on the current status of Open Radio Access Networks (Open RAN) and virtualized network environments, including potential obstacles to their development and deployment, and whether and how deployment of Open RAN-compliant networks could further the Commission's policy goals and statutory obligations. (WT Docket No. 21-63).

- On 5/27, Acting Commissioner Rosenworcel announced a Showcase for Open Radio Access Network Solutions.

GAO

GAO Reports: GAO has issued various reports related to 5G, including the FCC needs

comprehensive strategic planning to guide its efforts.

NTIA

NTIA BAA on Open RAN Technology: On June 3, 2021 NTIA's Institute for Telecommunications Science (ITS) issued the Broad Agency Announcement (BAA) to procure prototype or commercial-off-the-shelf (COTS) Open RAN equipment and software to be deployed in the ITS Communications Research and Innovation Network (CRAIN) to support ITS's testing of Open RAN equipment for evaluation of performance, inter-vendor interoperability, and standard maturity versus established RAN technologies.

White House

Executive Order on America's Supply Chains: On February 24, 2021, President Biden signed an Executive Order calling for a comprehensive review of domestic production, research and development capabilities, and the formulation of strategies to strengthen critical sectors. This effort is focused on the semiconductor industry, in part.

RECOMMENDATIONS

- Identify and support opportunities to partner with the international community to sign the existing template memorandum of understanding on 5G policy that includes support for 5G supply chain security and resiliency measures, vendor diversity, and open, interoperable networks.
- Increase collaboration with international partners to share information on domestic policy and regulatory updates, the development of standards-based open interfaces, and lessons learned for related engagement with industry.
- Enhance information sharing and best practices about grant programs, tax incentives, public financing, and other mechanisms to support vendor diversity.
- Support one-way or reciprocal trade delegations to highlight commercial opportunities and create deal making opportunities.

CONCLUSION

Widespread deployment of 5G will undoubtedly transform our essential networks and connectivity for years to come. The Internet of Things (IoT) landscape, smart cities, mobile money, and identity management technology are just a few areas that 5G will transform, highlighting the exigency of enhancing protection of these networks as well as the accompanying devices and applications. Though research and initiatives aimed at this goal are plentiful, there are also opportunities for increased collaboration amongst stakeholders to strengthen and expand defense solutions. This paper identified how federal, private sector, and international entities leading efforts related to 5G security can reduce duplicated pursuits, enhance sharing and communication, more efficiently deploy resources, and better utilize existing tools, programs, and legislation.

Moving forward, the 2021 Public-Private AEP Privacy and Security Implications of 5G Technology Team recommends DHS CISA maintain and update the above record of existing bodies of work in the four primary 5G focus areas in an easily accessible and centralized location. US federal agencies leading 5G risk mitigation efforts can leverage relationships with international partners to publicize the US bodies of work and establish further areas of collaboration not identified in this paper. The Privacy and Security Implications of 5G Technology Team will evaluate the feedback and impact of this paper to inform future 5G and wireless telecommunications efforts.

ANALYTIC DELIVERABLE DISSEMINATION PLAN

The following entities have been identified as recipients that would best benefit from receiving this deliverable:

- Cybersecurity and Infrastructure Security Agency (CISA)
- Federal Communications Commission (FCC)
- The White House; Office of Science and Technology Policy (OSTP), National Security Council (NSC)
- Department of Defense (DoD)
- National Science Foundation (NSF)
- National Institute of Standards and Technology (NIST)
- Cellular Network Providers (Verizon, AT&T, T-Mobile, Sprint, etc.)
- 5G Suppliers and Research Companies (Samsung, LG, Qualcomm, Nokia, Verizon, Cisco Systems, Ericsson, Dell, Microsoft, etc.)
- The Federal Bureau of Investigation (FBI)
- The Department of Commerce; FirstNet Authority
- Communications Sector Coordinating Council (CSCC)
- Information Technology Sector Coordinating Council (ITSCC)

DISCLAIMER STATEMENT: *This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and are the product of joint public and private sector efforts.*

2021
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Homeland
Security

2021
PUBLIC-PRIVATE
ANALYTIC EXCHANGE PROGRAM

Homeland
Security