Before the
UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In the Matter of	)	
The National Strategy to Secure 5G	)	
Implementation Plan	)	Docket No. 200521-0144
	)	
	)	

COMMENTS OF THE NATIONAL SPECTRUM CONSORTIUM

Sal D'Itri,
Chair

Randy Clark,
Vice Chair

National Spectrum Consortium

315 Sigma Drive
Summerville, SC 29486
P. 843.760.3344

June 18, 2020

Before the
UNITED STATES DEPARTMENT OF COMMERCE
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, D.C. 20230

In the Matter of	)	
The National Strategy to	)	
Secure 5G Implementation Plan	)	Docket No. 200521-0144
	)	

COMMENTS OF THE NATIONAL SPECTRUM CONSORTIUM

The National Spectrum Consortium ("NSC"),[1] a research, development, engineering and deployment organization that is actively working with government, academia and industry to solve the nation's toughest challenges related to enabling 5G, is pleased to offer, via these comments, strategies the Administration can employ in its implementation plan (the "Implementation Plan") to accelerate rollout of 5G infrastructure consistent with the President's National Strategy to Secure 5G.[2]

Building on the Administration's desire to "work aggressively with the private sector . . . to foster and promote the research, development, testing and evaluation of new technologies and architectures that advance the state of the art technology for 5G and beyond",[3] NSC makes the following initial recommendations for the Implementation Plan:

1. The Administration can and should view NSC as an essential tool in the Implementation Plan. The Implementation Plan should leverage the government – private sector nexus fostered by NSC around 5G, and leverage NSC's capacity for advanced wireless research, prototyping, testbeds, and partnerships to facilitate technology development and deployment for 5G and beyond. The Administration can count among its assets NSC's unique mix of non-traditional, small commercial

[1] *See* https://www.nationalspectrumconsortium.org/.

[2] On March 23, 2020, the President signed into law the Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129, 134 Stat. 223-227 (2020) (the "Act"). On this same day, the White House published The National Strategy to Secure 5G of the United States of America, March 2020, available at https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf (the "WH Secure 5G Strategy"). As NTIA notes in its Public Notice seeking comment on the National Strategy to Secure 5G Implementation Plan, the Act requires the development of an Implementation Plan within 180 days of enactment. 85 Fed. Reg. 32016 (May 28, 2020) (the "NTIA Public Notice"). That Implementation Plan is the subject of these comments.

[3] WH Secure 5G Strategy at 2.

vendors, academic institutions and large DoD contractors to establish US leadership on the global stage, including through partnering with international industry and standards setting organizations;

2. In order to best motivate the domestic 5G ecosystem to increase 5G research and testing, the Implementation Plan should utilize an "Other Transaction Authority," such as NSC, to provide targeted government funding for private sector research on 5G technologies; and

3. The Implementation Plan should prioritize research and development of dual-purpose technologies and standards that will meet 5G needs for both government and private sector users, leading to a more secure and robust equipment and services ecosystem for 5G in the United States.

The United States has made great strides in developing 5G technologies, deploying 5G networks, and offering 5G services. The Implementation Plan should drive articulation and implementation of a beyond-5G vision. NSC encourages the Administration to think towards a beyond-5G future and scope its Implementation Plan to focus not just on 5G, but on shaping the requirements for future generations of wireless technologies.

I. NSC Can and Should Serve as An Essential Tool in the Administration's Implementation Plan, Facilitating 5G Research, Prototyping, and Planning.

NTIA asks in its Public Notice how the U.S. Government can "best foster and promote the research, development, testing and evaluation of new technologies and architectures."[4] In NSC's view, the Administration can best foster and promote 5G for the United States by leveraging the organizations, research capabilities and partnerships NSC encompasses as an essential tool in the Implementation Plan. The below provides background on NSC and describes its ongoing critical 5G research, prototyping, and testbeds.

A. Background on NSC.

NSC was formed in 2015 to facilitate a five-year, $1.25 Billion, Section 815 Prototype Other Transaction Agreement ("OTA") with the Department of Defense ("DoD"), executed through the Office of the Deputy Assistant Secretary of Defense, Emerging Capabilities and Prototyping. NSC plays an important role in the development of new wireless technologies, fostering collaboration between the government and the private sector to identify critical needs in wireless systems and services, and developing effective solutions. Indeed, NSC's

[4] NTIA Public Notice at 32017.

mission is to foster collaboration among government, industry and academia to identify, develop, prototype and demonstrate enabling technologies that will broaden both government and commercial access to, and use of, spectrum and technologies for 5G and beyond.

The DoD is deeply involved in evaluating and researching 5G technologies through its OTA with NSC, in large part because of the vendor diversity and expertise within NSC's membership. NSC recognized from the beginning that leadership on advanced spectrum, radio and networking technologies, artificial intelligence, and cybersecurity is found in a variety of settings – small start-up technology companies, major telecommunications carriers and vendors, traditional government contractors, and academia. NSC currently counts 359 organizations within its membership (a full list is attached in Appendix A), and includes responsible global development partners and allies, trusted government contractors and global wireless equipment vendors. NSC members are required to be cleared through the Defense Logistics Agency Joint Certification Program, which allows members to access unclassified export controlled technical information.

Beyond its diverse vendor community, NSC resources include our Nation's leading technologists, engineers, scientists, manufacturers, and program managers from industry, academia, and government. These individuals already are working together through NSC to solve the toughest problems facing the nation with regard to 5G and future radio and network technologies, accessing scarce spectrum resources and securing our wireless networks. NSC's efforts are enabling the development and demonstration of dynamic spectrum access and sharing technologies on a timescale far more efficient than traditional approaches, facilitating early and impactful action.

Success for NSC has been driven by bringing all these diverse players together to help facilitate and accelerate technology transformation. NSC agrees with the Administration that promoting vendor diversity and fostering new supply chains and market competition will be critical to the success for 5G and beyond.[5] In view of all its ongoing 5G work, its broad and diverse membership, and its research and partnerships, NSC hopes that the Administration will include working with NSC as an essential tool in the 5G Implementation Plan to stimulate additional research, development, and prototyping through the NSC OTA.

[5] *See*, WH Secure 5G Strategy at 6; NTIA Public Notice at 32017.

B. Examples of Ongoing 5G Research, Prototyping and Testbeds.

NSC has, to date, granted individual awards for DoD projects ranging from $360,000 to $45 million. Many of the 60 awarded projects[6] are essential to 5G success, including, just by way of example - prototyping of new radio hardware and elements of 5G testbeds, design and operation of a localized, private 5G mobile cellular network, 5G network enhancements, monitoring for spectrum coexistence and sharing, integrating network intelligence via machine learning, and advancing phased array and MIMO antenna technologies.

Through NSC, the DoD recently released the following 5G Requests for Prototype Proposals ("RPPs"), calling on NSC members to develop technology related to dynamic spectrum sharing that is critical for 5G, at testbeds established at Hill Air Force Base and a Utah Test and Training Range:

- NSC-20-2070 – 5G Prototype Testbed to design, construct and operate a localized, private full scale 5G mobile cellular network in order to evaluate the impact of the 5G network on airborne radio systems.

- NSC-20-2080 – 5G Prototype Enhancements specifically to enhance dynamic spectrum sharing and spectrum co-existence capabilities.

- NSC-20-2090 – 5G Prototype Applications to design, construct and deploy a Spectrum Coexistence and Sharing (SCS) system to identify and demonstrate deployable SCS.

In addition, earlier this year, through NSC, DoD issued two 5G Smart Warehouse RPPs for technology development at the Marine Corps Logistics Base in Albany, Georgia and Naval Base San Diego, and a third RPP for Augmented Reality/Virtual Reality prototypes at Joint Base Lewis-McChord in Washington state. All NSC members in good standing are permitted to submit proposals in response to RPPs, and there is broad participation across the membership.

NSC is well-positioned to offer the Administration not only implementation advice, but also offer NTIA a ready structure to continue fostering and promoting federal/non-federal research on 5G, afford access to the Nation's top scientists, provide valuable research results, and provide avenues and diverse partners for further research that will ensure a successful 5G Implementation Plan.

---

[6] *See, National Spectrum Consortium, Project Awards, available at https://www.nationalspectrumconsortium.org/project-awards/.*

II. The Administration's Implementation Plan Should Specify an OTA such as NSC to Provide Targeted Government Funding for Private Sector Research on 5G.

In order to best motivate the domestic 5G ecosystem to increase 5G research and testing,[7] and provide an avenue to use the buying power of the federal government as suggested by the President,[8] NSC recommends strongly that the Administration consider using an OTA such as NSC to facilitate research in its 5G Implementation Plan.

An OTA, also known as an "Other Transaction Agreement" or "Other Transaction Authority," is a streamlined contracting vehicle that assists industry in bringing innovative research findings and state-of-the-art prototypes to the federal government. Using an OTA to advance our nation's goals related to 5G will satisfy many of the 18 required actions set forth in the *Secure 5G and Beyond Act of 2020*.[9] OTAs such as NSC can provide evaluation of domestic suppliers of 5th and future generations of wireless communications equipment, they can and already do engage with the private sector about 5G production issues, they share information about systems and infrastructure, they participate in standards' setting bodies, they enable joint testing environments, and they

---

[7] NTIA asks in its Public Notice, "What steps can the U.S. Government take to further motivate the domestic-based 5G commercial ecosystem to increase 5G research, development and testing." NTIA Public Notice at 32017.

[8] WH Secure 5G Strategy at 1.

[9] For example, an OTA could support all of the following actions from the Act: (3) An evaluation of available domestic suppliers of 5th and future generations wireless communications equipment and other suppliers in countries that are mutual defense allies or strategic partners of the United States and a strategy to assess their ability to produce and supply 5th generation and future generations wireless communications systems and infrastructure; (8) A plan for engagement with private sector communications infrastructure and systems equipment developers and critical infrastructure owners and operators who have a critical dependency on communications infrastructure to share information and findings on 5th and future generations wireless communications systems and infrastructure equipment standards to secure platforms; (9) A plan for engagement with private sector communications infrastructure and systems equipment developers to encourage the maximum participation possible on standards-setting bodies related to such systems and infrastructure equipment standards by public and private sector entities from the United States; (12) A plan for joint testing environments with mutual defense treaty allies, strategic partners, and other countries to ensure a trusted marketplace for 5th and future generations wireless communications systems and infrastructure equipment; (13) A plan for research and development by the Federal Government, in close partnership with trusted supplier entities, mutual defense treaty allies, strategic partners, and other countries to reach and maintain United States leadership in 5th and future generations wireless communications systems and infrastructure security, including the development of an ongoing capability to identify security vulnerabilities in 5th and future generations wireless communications systems. *See* Act at Sec. 3(d).

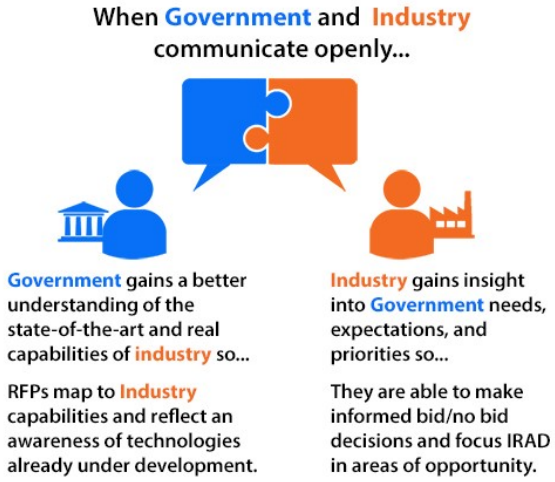
enable research and development in close partnership with the federal government, trusted suppliers and strategic partners.

Congress created the first OTA as a contractual tool for NASA to acquire and apply breakthrough technologies at the advent of the space race. Today, OTAs enable fast development, prototyping, and acquisition of critically needed technologies in areas as diverse as armaments, satellites, medical devices, and electromagnetic spectrum technologies. Unlike using the Federal Acquisition Regulations, using an OTA-based consortium model to advance 5G and future wireless implementations will allow government and industry to communicate more openly, from requirement generation to the proposal stage, including the following benefits:

- An OTA can afford greater technology and prototype acquisition speed, getting 5G solutions to market sooner;

- An OTA emphasizes engaging a diverse range of technology suppliers of all sizes, casting a wider net for capturing 5G ideas and innovations; and

- OTAs enable faster contracting through long-term agreements between industry and government that establish baseline terms and conditions (with the flexibility for negotiated modifications on a project-by-project basis).



Working through an OTA such as NSC will allow for government – private sector collaboration across all stakeholders, including smaller and non-traditional contractors that are developing new technologies and creating test beds alone, or in combination with existing contractors or service providers. As recognized by the White House, collaboration among a diversity of companies,

academics, and government users, has generated, and will continue to generate, fruitful innovations for 5G and beyond.

In NSC's view, the nation's 5G implementation plan would clearly benefit from relying on an OTA as a vehicle for critical research, development, and prototyping. OTAs represent good government in action by promoting competition among large, traditional research and development providers, academic institutions, and small and nontraditional suppliers, driving innovation across the entire ecosystem, and accelerating secure 5G deployment for all.

III. The Administration's Implementation Plan Should Prioritize Research and Development of Dual-Purpose Technologies and Standards That Will Meet 5G Needs For Both Government and Private Sector Users, and Will Lead to a More Secure and Robust Equipment and Services Ecosystem.

NTIA asks for recommendations on "areas of research and development" the US. Government should prioritize for 5G. [10] NSC strongly recommends that the Administration's Implementation Plan prioritize research and development of dual-purpose technologies for 5G that will satisfy both government and commercial needs.

Although the goals for government use of 5G and commercial use of 5G do not always align, such alignment of goals is not essential. By design, 5G technologies can meet myriad commercial and federal goals and use cases, without significant modification.[11] Commercially, 5G technologies can enable fixed and mobile services, the Internet-of-things, vehicle communications, smart grid, and countless other services. By nature, these technologies can serve similar purposes to meet federal needs. These technologies are fundamentally focused on providing wireless connectivity for any application, with any bandwidth requirement, and any quality of service demands. Collaboration among government, industry and academia to develop these technologies will intrinsically lead to improved capabilities and utilities for 5G across both commercial and government uses, and will accelerate development of 5G and future wireless technologies for our nation.

---

[10] NTIA Public Notice at 32017.

[11] As NTIA is aware, 5G differs in character significantly from prior networking technologies due to its ambitious reach into societal and economic spheres well-beyond mere network provisioning and attendant services by an operator. However, the advent of 5G networks and technologies, combined with increased intensity of spectrum sharing between federal and non-federal users, has changed this paradigm to the benefit of both federal agencies and the commercial sector.

There is no question that the United States' private technology and wireless sectors are leaders at developing and deploying new technologies and services for the private sector, including 5G, but the government has a critical role to play to influence development vectors as an early adopter. The alignment of government and private sector on 5G is clear in some other countries. In China, for example, the government has long aligned government interests with private industry and academia into a unified alliance to enhance their country's competitiveness in 5G.[12] The Administration should consider in its Implementation Plan how a more unified approach by the government, commercial and academic sectors with respect to 5G and future wireless technologies will enhance United States' pre-eminence for the long-term horizon.

Government involvement to prioritize and encourage the development of dual-use technologies will help foster an even more robust domestic wireless equipment ecosystem, in two key ways. First, government sponsored research and development can provide capital for fundamental research from small business and academia that might be too attenuated from commercialization for private sector investment. Second, the combination of the government and private sector markets creates one extremely large market, better able to support a larger, more diverse and more competitive ecosystem.

For all these reasons, NSC recommends that the Administration's Implementation Plan prioritize research and development of dual-purpose 5G technologies, including (but not limited to) the three technologies and standards highlighted below: (1) 5G future wireless security; (2) spectrum sharing; and (3) baseband technologies and standards.

A. <u>5G and Future Wireless Network Security</u>.

As the President's *National Strategy to Secure 5G* recognizes, 5G security looms as a major issue that must be addressed.[13] In the view of NSC, the government has a particularly critical role to play with respect to 5G security. The government can help push research and development for dual-purpose network security and trust to ensure that private and public sector 5G implementations are just as secure as 5G implementations for government users.

---

[12] "The Chinese government is implementing a concerted strategy of civil-military fusion through the sale and deployment of 5G telecom systems . . . ." *The U.S. Must Treat China as a National Security Threat to 5G Networks*, Klon Kitchen, Technology Report, The Heritage Foundation (April 16, 2019), available at https://www.heritage.org/technology/report/the-us-must-treat-china-national-security-threat-5g-networks.

[13] "5G infrastructure must be secure and reliable to maintain information security and address risks to critical infrastructure, public health and safety, and economic and national security." WH Secure 5G Strategy at 1.

NSC believes a "zero trust" model could be used as a fundamental security strategy throughout the 5G supply chain.[14] The U.S. Government has adopted a zero trust security standard for their communications networks, and some commercial users also are adopting the zero trust standard.

NSC and its members are working at the leading edge of zero trust, setting up reference architectures and requiring that each 5G testbed run by NSC members include implementation of zero trust security. The Administration's Implementation Plan should require commercial industry to work with the U.S. Government on zero trust architectures that will enable deployment of zero trust technology in each private, public and government 5G implementation. The Administration also should think beyond 5G and consider security approaches for future wireless technologies that are still in very early stages of development, in order to build security into the technologies and standards from the start.

In addition to zero trust as a foundational element of 5G security, NSC recommends that the Administration task the National Institute of Standards and Technology ("NIST") to develop a risk-based model for 5G and future wireless technologies and services. Insisting on development of dual-purpose security technologies for 5G will ensure identification of core security principles that can be implemented in all 5G networks in America.

B. <u>Spectrum Sharing</u>.

Spectrum sharing is another area in which research should focus on dual-purpose technologies that will satisfy both government and commercial users. Spectrum sharing is a critical policy and technology solution that ensures that access to the limited spectral resource does not need to be a zero sum game. Through spectrum sharing technology, government and commercial users can share spectrum resources, protecting mission critical operations and making spectrum available to other users when and where the spectrum is available.

---

[14] As NTIA is likely aware, a zero-trust security solution constantly evaluates trust every time a device or user requests access to a resource. This method prevents attackers from exploiting vulnerabilities in the perimeter to gain entry and then access confidential data and applications. The NIST, in its current draft of standards for a zero trust architecture, defines zero trust as a "cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated." NIST, Zero Trust Architecture, Draft (2nd) NIST Special Publication 800-207, available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207-draft2.pdf. NIST notes that there is a distinction between zero trust and zero trust architecture: "Zero trust provides a collection of concepts and ideas designed to reduce the uncertainty in enforcing accurate, per-request access decisions in information systems and services in the face of a network viewed as compromised." *Id.* Zero trust architecture "is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies." *Id.*

As spectral resources have become ever more constrained, spectrum sharing tools have been developed to facilitate enhanced and efficient commercial and federal spectrum sharing. Although these solutions can allow disparate systems to coexist on the same frequency bands, the task is greatly enhanced with the types of systems that commercial and federal users share, whether in application, standard, or implementation.

Targeted research and development of dual-purpose technologies, for spectrum sharing for government and commercial users, will allow better utilization of this critical natural resource for all spectrum users which is essential for 5G success.

C. <u>Standards</u>.

As the Administration has recognized, standards development is a critical step for the 5G wireless ecosystem, both for the government and the private sector.[15] Standards-setting work is a collaborative process that should align efforts across vendors, service providers, and countries to efficiently develop robust and interoperable global technologies.

Substantial standards-setting work for 5G is ongoing in organizations such as the Third Generation Partnership Project ("3GPP") and its North American Organizational Partner, the Alliance for Telecommunications Industry Solutions ("ATIS"), as well as the Institute of Electrical and Electronics Engineers ("IEEE"), all of which serve as global standards-setting bodies for the wireless ecosystem. To date, agencies in the United States' federal government have largely avoided direct or indirect participation in such efforts. As a result, the standards may not fully reflect or satisfy the needs of federal government users. The Administration is right to focus on this issue.

NSC recommends the Administration include in its Implementation Plan a method for the U.S. Government to collaborate on robust industry-led, dual-purpose standards development for 5G, and help influence the development of 5G standards that will, by design, accommodate some, if not all, federal and commercial needs. This type of collaboration should leverage U.S. Government participation in 3GPP's North American Organizational Partner ATIS, recognizing

---

[15] WH Secure 5G Strategy at 6 ("The United States Government will work to preserve and enhance United States leadership on 5G in relevant organizations that set standards in concert with the private sector . . . This will include efforts such as expanding Federal interagency coordination, participation and influence in standards-setting organizations.") NTIA also highlighted this issue in its Public Notice: "How can the U.S. Government best encourage and support U.S. private sector participation in standards development for 5G technologies." NTIA Public Notice at 32017.

the span across all different types of standards groups, and reflecting the reality that the wireless ecosystem is not a monolith, but a collection of different standards from different groups, from mobile wireless, to wirelines networks, and components in between.

In NSC's view, developing joint, dual-purpose technologies and standards for many, if not most, components of the 5G ecosystem, including security, spectrum sharing and wireless standards, will hasten development of a more secure and robust 5G ecosystem for all.

IV. Conclusion.

As described in these comments, NSC feels confident that through its research and prototyping activities, it can serve the Administration in facilitating "the accelerated development and rollout of 5G infrastructure in the United States and with our international partners, and lay the groundwork for innovation beyond 5G."[16] The Administration can and should think of NSC as an essential tool in the Administration's Implementation Plan, facilitating government-private sector collaboration, 5G research, prototyping, and network planning and testing. In the view of NSC, the Implementation Plan should drive articulation and implementation of a beyond-5G vision utilizing NSC's unique mix of vendors, ongoing 5G work, capabilities, partnerships and research projects to facilitate accelerated 5G deployment.

Beyond this, NSC encourages the Administration in its Implementation Plan to utilize an OTA such as NSC to provide targeted government funding for private sector research on 5G technologies, and to focus on development of dual-purpose technologies and standards that will meet 5G needs for both government and private sector users, leading to a more secure and robust 5G ecosystem. In combination, use of the strategies suggested by NSC will help the United States accelerate and lead in 5G and ensure a secure and successful future for 5G and technologies beyond 5G.

[16] NTIA Public Notice at 32017.

Appendix A:
List of Active NSC Members

AASKI Technology, Inc.
Abside Networks, Inc.
Accenture Federal Services LLC
Adjacent Link LLC
Advanced Ground Information Systems, Inc.
AECOM Management Services
Aeronix, Inc.
Aether Argus Inc
AiRANACULUS
Alion Science and Technology Corporation
All Purpose Networks Inc.
American Systems Corporation
ANDRO Computational Solutions, LLC
Anokiwave, Inc.
Ansys, Inc.
Antenna Research Associates, Incorporated
AnTrust
Applied Technology Associates
Aqsacom Incorporated
Arizona State University
Aspen Consulting Group
Associated Universities, Inc.
Astrapi Corporation
AT&T Corp.
AT&T Government Solutions, Inc
ATDI Government Services, LLC
Athena Technologies, LLC
Augmntr, Inc.
Augustine Consulting, Inc (ACI)
AuresTech Inc
AVANTech Inc
AVT Simulation
Axellio Inc.
BAE Systems Information and Electronic Systems Integration Inc.
Ball Aerospace & Technologies Corp
BANC3, Inc
Baylor University
Bear Systems
Beatty and Company Computing Inc.
BlackHorse Solutions Incorporated
Blue Danube Systems, Inc.
Boeing Company
Booz Allen Hamilton Inc.
Bridge 12 Technologies
BridgeSat Inc.
Brigham Young University
Cambium Networks, Inc
Catholic University of America, The
Celona Inc
CesiumAstro
CGI Federal Inc.
Chesapeake Technology International Corporation
CIPHIR-TM, LLC
Cisco
Chesapeake Technology International Corporation
CIPHIR-TM, LLC
Cisco
Cobalt Solutions Inc.
Cobham Advanced Electronic Solutions
Cole Engineering Services, Inc. (CESI)
Collins Aerospace
Colorado Engineering Inc.
Columbia University
CommScope Technologies LLC
Comsearch
ComSovereign Corp.
Comtech Mobile Datacom Corporation
Concurrent Technologies Corporation
Conductive Composites Company
Consolidated Resource Imaging LLC (CRI)
Corner Alliance, Inc.
Corning Specialty Materials
Corvus Consulting, LLC
Creative Digital Systems Integration, Inc.
CRFS Inc.
Cubic Defense Applications, Inc.
Cybernet Systems Corporation
DEEPSIG Inc.
Dell Federal Systems L.P.
Deloitte Consulting, LLP
Digital Global Systems, Inc
DTC Communications, Inc.
Dynetics, Inc.
EFW, Inc. (Elbit)
Eigen Wireless
Electronic Design and Development Corp (ED2)
Enveil, Inc.
EPIC Scientific
Epiq Solutions
EpiSys Science, Inc.
Epsilon Systems Solutions, Inc.
Erebus Solutions Inc.
Ericsson, Inc.
Eridan Communications, Inc.
eSimplicity, Inc.
EWA Government Systems Inc.
Ewing Engineered Solutions
Expression Networks LLC
Federated Wireless
Fenix Group, Inc.
Florida Atlantic University
Freedom Technologies, Inc.
Frequency Electronics, Inc
Garou Inc.
GATR Technologies
GBL Systems Corporation
GE Research
General Dynamics Information Technology, Inc.

General Dynamics Mission Systems, Inc. (GDMS)
GenXComm, Inc.
Geon Technologies, LLC
George Mason University
Georgia Tech Applied Research Corporation
GIRD Systems Inc.
Global Technical Systems
Gonzaga University
GPS Source, Inc.
GreenSight Agronomics, Inc.
Hanwha International LLC
Harris Corporation
Harris Corporation RF Communications Division
HawkEye 360, Inc.
Herrick Technology Laboratories, Inc
Hewlett Packard Enterprise Company (HP)
Honeywell International, Inc.
HRL Laboratories, LLC
Huckworthy LLC
Hughes Network Systems, LLC
IAI, LLC
IERUS Technologies, Inc.
IJK Controls LLC
IMSAR LLC
InCadence Strategic Solutions
Indiana Microelectronics, LLC
Indiana Tool & Mfg. Co., Inc. DBA ITAMCO
Innovative Power LLC
Institute for Building Technology and Safety (IBTS)
Integration Innovation Inc. (i3)
Intel Federal LLC
Intelligent Automation, Inc.
Intelligent Fusion Technology, Inc.
InterDigital Communications
Intuitive Research and Technology Corporation
IOMAXIS, LLC
iPosi Inc
Iron Bow Technologies, LLC
IT Consulting Partners, LLC (ITC)
Jacobs Technology
Janus Communications
JANUS Research Group, LLC
JC3 LLC
Johns Hopkins University Applied Physics Laboratory
Key Bridge Wireless LLC
Keysight Technologies, Inc
KinetX, Inc.
Knowledge Based Systems, Inc
Knowledge Management Inc.
KPMG LLP
Kumu Networks
L3 Communications Systems East
L3 Communications Systems West
L3 Communications Telemetry West
L3 Technologies
Laulima Systems
Leidos, Inc.
LGS Innovations (CACI)
LinQuest Corporation
LocatorX, Inc.
Lockheed Martin Corporation
Logistics Management Institute (LMI)
LS telcom Inc.
Mavenir Systems, Inc.
MaXentric Technologies, LLC
McKean Defense Group
MegaWave Corporation
Metamagnetics Inc.
Microsoft Corporation
Mimyr, LLC
Mississippi State University
MixComm, Inc.
Mobilestack Inc
Motorola Solutions, Inc.
MW Ventures LLC, DBA Social Mobile
National Instruments Corporation
NEC Corporation of America
NetApp, Inc.
New Mexico State University
NewEdge Signal Solutions LLC
Nexagen Networks Inc
NextGen Federal Systems, LLC
Nokia
North Carolina State University
Northeast Information Discovery, LLC (NEID)
Northeastern University
Northern Arizona University
Northrop Grumman Systems Corporation, Electronic Systems
NorthWest Research Associates, Inc.
Novaa Ltd
Novowi LLC
NTS Technical Systems
Numerati Partners, LLC
Nuvotronics, Inc.
Oceus Networks Inc.
Old Dominion University Research Foundation
Omnispace
Opex Systems LLC
ORSA Technologies, LLC
OST, Inc.
Otava, Inc
Pacific Antenna Systems LLC
Pacific Star Communications, Inc.
Palo Alto Networks Public Sector, LLC
Parallel Wireless, Inc.
Parry Labs, LLC
Parsons Government Services Inc.
Pathfinder Wireless Corp
Peraton, Inc.
Peregrine Technical Solutions, LLC
Persistent Systems, LLC
Perspecta Labs

Phase Sensitive Innovations, Inc.
Photonic Systems Inc.
Physical Optics Corporation
Pi Radio Inc.
Pinnacle Solutions, Inc.
PlusN, LLC
Pn Automation, Inc.
Polaris Alpha Advanced Systems, Inc.
Power Fingerprinting Inc.
Purdue University
Q Networks, LLC
Qorvo Texas, LLC
QRC Technologies
QuayChain, Inc
Qubitekk, Inc
Radiance Technologies, Inc.
Rajant Corporation
Rakuten USA, Inc.
RAM Laboratories, Inc.
Raven Wireless, LLC
Ravenswood Solutions
Raytheon Company
RDA Technical Services (Robert Doto Associates, LLC)
ReFirm Labs, Inc.
Resonant Sciences LLC
Rivada Networks LLC
Riverside Research Institute
RKF Engineering Solutions, LLC
Roberson and Associates LLC
Rohde & Schwarz USA, Inc.
RT Logic
RunSafe Security, Inc.
Rutgers, The State University of New Jersey
S2 Corporation
SA Photonics, Inc.
Sabre Systems, Inc.
Samsung Research America, Inc.
Scientific Research Corporation
SecureG, Inc
Selex Galileo Inc
Sentar, Inc.
Sentrana
Shared Spectrum Company
Shipcom Federal Solutions, LLC
Signal Hound, Inc.
Signal Point Systems, Inc.
Signal Processing Technologies, Inc.
Silvus Technologies, Inc.
Simba Chain, Inc.
Skylark Wireless, LLC
SOLUTE, Inc.
Southern Methodist University
Southern Research
Southwest Research Institute
Space Exploration Technologies Corp. (SpaceX)
Spectral Labs Incorporated
Spectrum Bullpen, LLC
Spirent Communications, Inc.
Sprint Solutions, Inc.
SRC Inc.
SRI International
SSC Innovations
Starry, Inc.
Stevens Institute of Technology
Strategic Data Systems, Inc.
Stratom, Inc.
Summation Research, Inc.
Syncopated Engineering Inc
Synoptic Engineering, LLC
Systems & Technology Research, LLC
T2S, LLC
Technology Service Corporation (TSC)
Technology Unlimited Group
Terry Consultants, Inc
Texas A&M Engineering Experiment Station
Thales Defense & Security, Inc.
The Aerospace Corporation
The Charles Stark Draper Laboratory, Inc.
The Kenjya-Trusant Group, LLC
The University of Texas at Dallas
Thinklogical, LLC
Tilson Technology Management Inc
TLC Solutions, Inc.
T-Mobile USA Inc.
Toyon Research Corporation
Trabus Technologies, Inc.
TrellisWare Technologies, Inc.
Trex Enterprises Corporation
Tribalco, LLC
TrustComm, Inc.
Two Six Labs, LLC
Ultra Communications, Inc.
Undergrid Networks, Inc.
United Technologies Research Center (UTRC)
University at Buffalo
University at Albany
University of Arizona - Electrical and Computer Engineering
University of Colorado Boulder
University of Illinois
University of Kansas Center for Research, Inc.
University of Mississippi
University of Notre Dame (Wireless Institute)
University of Oklahoma
University of South Carolina
University of Texas at San Antonio
University of Virginia
University of Washington
US Ignite, Inc.
Vectrona, LLC
Vectrus Mission Solutions Corporation
Veritech, LLC
Verizon Wireless

Verus Research
ViaSat Inc.
Virginia Tech Applied Research Corporation (VT-ARC)
VIStology Inc.
Vmware, Inc
W5 Technologies, Inc.
WaveLink, Inc.
Whitney Strategic Services, LLC
William Marsh Rice University
Wind Talker Innovations Inc.
Wireless at Virginia Tech
Wireless Research Center of North Carolina
World Wide Technology, Inc. (WWT)
X-COM Systems LLC
XCOM-LABS, INC.
Zoic Labs, LLC
Zylinium Research LLC