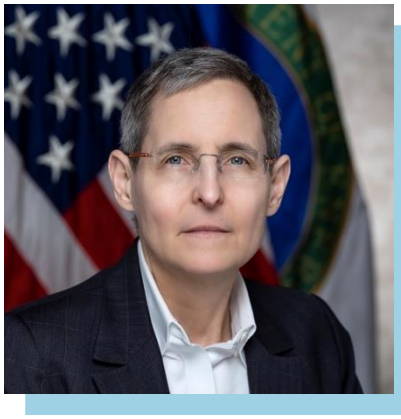
U.S. DEPARTMENT OF ENERGY
Office of the Chief Information Officer

Advanced Wireless Strategy

U.S. DEPARTMENT OF ENERGY

Table of Contents

Message From the Chief Information Officer



The Department of Energy (DOE), together with its National Laboratories, have developed this strategy as a follow-on to the 2021 *5G Research, Development, Test, Evaluation and Training Catalog.* This strategy identifies priority activities for how DOE will approach implementing the *National Strategy to Secure 5G* in ways relevant to its missions.

Fifth generation (5G) and beyond wireless communication technologies promise orders of magnitude improvements in throughput, connectivity, and reduced latency, and will be a primary enabler of our Nation's prosperity and security. This new technology will enable vastly more smart devices to connect to the Internet, thereby accelerating the digital transformation that is already underway. Devices from vehicles to control and communication systems in the grid may become more capable through inclusion of new edge computing and cloud services, algorithms, and applications when connected to these advanced wireless networks. Advanced wireless networks are anticipated to spur innovation and provide consumers, businesses, governments, and DOE missions with remarkably faster networks, transforming the way we live, work, and communicate.

Despite the aforementioned benefits, this technology also introduces significant risks that can threaten DOE missions as well as our national and economic security. Given the complexity of the advanced wireless infrastructure, even inadvertent vulnerabilities may be difficult to detect and prevent. For these reasons, our deployment of advanced wireless technology solutions must incorporate effective protections for existing federal and non-federal licensed radio spectrum users and prioritize security considerations by avoiding untrusted and unreliable suppliers.

Emerging advanced wireless technology offers significant growth opportunities and capabilities to all phases of DOE research and development, from basic and applied research through application and deployment. These capabilities are also anticipated to provide a wide range of advantages across DOE mission activities. The DOE enterprise has extensive facilities and expertise relevant to advanced wireless technology and is already engaged in innovative scientific research and applied testing for advanced wireless security, network resiliency, energy grid applications, and spectrum management. These efforts are in concert with, and in support of, the whole-of-government and whole-of-nation effort on 5G.

DOE is committed to working with our partners and stakeholders to implement the key pillars of this strategy needed to ensure the development of secure advanced wireless technology for our mission and our Nation.

Ann Dunkin, P.E.

Executive Summary

Advanced wireless networks and communication technologies have the potential to positively transform the way DOE carries out its key missions, including securing the grid; combating climate change; expanding broadband to remote and underserved locations; promoting scientific research and discovery; securing the nuclear enterprise; and creating clean energy jobs**.** DOE's contributions in the advanced wireless space will further U.S. efforts to achieve global leadership in telecommunications as well as enhance the resiliency of our national critical infrastructure.

However, this rapidly evolving technology also introduces significant challenges that negatively impact DOE's ability to leverage advanced wireless for its missions. Some key technological challenges include but are not limited to an increased need for dedicated spectrum resources; the need to understand and respond to threats and vulnerabilities to our advanced wireless infrastructure and supply chains; and the need for standards that provide sufficient flexibility with maximum security protections. On the policy and operational side, insufficient investment, resourcing, and collaboration have hampered broad research and development efforts that could provide solutions to meet both enterprise-wide mission and national needs. To take advantage of the transformative capabilities offered by 5G and beyond, DOE will need to accelerate its investment in research, development, and deployment of advanced wireless, while ensuring such deployments are secure and reliable.

With input from throughout the enterprise, DOE has identified recommendations across five distinct strategic pillars to overcome some of its biggest challenges, fill key gaps, and help accelerate our advanced wireless work. Together, these strategic pillars will help prioritize and guide activities critical to achieving leadership in advanced wireless implementation by:

1. Advancing the development of capabilities to further secure our access to adequate spectrum.
2. Understanding and mitigating threats and vulnerabilities through enhanced monitoring techniques and robust implementation of security measures and supply chain risk management.
3. Advancing the energy mission through grid modernization and securing the path to Net Zero.
4. Supporting communications equity by using our assets to develop and deploy broadband capability to rural and underserved communities.
5. Increasing collaboration and coordination with internal and external partners and stakeholders to leverage capabilities and share discoveries and best practices.

With its legacy of innovation, research and development, computational infrastructure, and thirst for accelerating scientific discovery, DOE and its National Laboratories, through implementation of this advanced wireless strategy, are uniquely positioned and fully committed to helping our Nation seize the opportunity to lead the world in this critically important technology.

Strategic Context

Advancing DOE Missions

The U.S. energy infrastructure fuels the economy of the 21st century, and that infrastructure relies extensively on technology for extraction, storage, movement, and delivery of energy supplies. Without a stable energy supply, health and welfare are threatened, and the U.S. economy cannot function. Presidential Policy Directive 21 identified the Energy Sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. Advanced wireless has the potential to play a key role in almost every DOE mission area, including important contributions to Administration priorities such as combating climate change; securing the grid; supporting communications equity by reducing the digital divide and expanding broadband to remote and underserved locations; securing the nuclear enterprise and protecting national security; and creating clean energy jobs. With its high bandwidth and low latency, the use of 5G and beyond will significantly improve the frequency usage, operational communications, emergency preparedness, and site security across the DOE enterprise including the 17 National Laboratories and the four Power Marketing Administrations (PMAs).

Combating climate change

Advanced wireless has the potential to lead to profound improvements for sensors, controls, and other distributed technologies to advance clean energy deployment and maximize the efficiency of the energy sector to achieve Net Zero goals. Advanced wireless will also enable new continuous data sources to further climate research and potentially impact the way we gather and transfer data, enhancing the analysis of climate problems and solutions. Low latency communications are necessary for distributed energy resources such as photo-voltaic and technology that requires the use of inductors to form a grid.

Securing the grid

As advanced wireless becomes part of the energy grid, it needs to be properly safeguarded. For utilities, advanced wireless offers the opportunity to eliminate resource inefficiencies by automating power generation, distribution, storage, and control systems. A data-driven grid is more resilient, but much more vulnerable as it creates more routing points and edge devices that must be secured. DOE's advanced wireless research activities will help enable development of security standards, innovation for spectrum allocation and sharing, enhancement of test beds for security experimentation, and development of security solutions for private communications networks.

Supporting communications equity by reducing the digital divide

The deployment in rural and remote areas of 5G-powered data networks, sensors and other devices, command and control systems, autonomous reconfiguration capabilities, and even the potential for harnessing the grid itself as a data network, will help connect underserved communities (including in many of the communities where National Laboratories and/or extensive power grid infrastructures are located) to the next generation of both clean energy sources as well as reliable and fast broadband internet. Using our national energy infrastructure, rights of way, and energy control backbone to help deploy robust and secure 5G networks serving historically rural, underserved, and unserved areas promotes equity by making sure those who have been denied access to the latest technologies and networks for far too long will be the first to benefit from its potential.

Securing the nuclear enterprise and protecting national security

The National Nuclear Security Administration (NNSA) maintains and enhances the safety, security, and effectiveness of the U.S. nuclear weapons stockpile; works to reduce the global danger from weapons of mass destruction; provides the U.S. Navy with safe and militarily effective nuclear propulsion; and responds to nuclear and radiological emergencies in the United States and abroad. Advanced wireless has the potential to promote updates to aging infrastructure and unique use cases to the mission where environments have low-bandwidth and high latency. It could also improve real-time scenarios where critical information is required for mission success. Even though there are many advancements this technology can provide, NNSA must take a risk-based approach toward its development to ensure that cybersecurity is embedded at every layer. Using an effective mix of technology, policy, and risk management practices will enable the enhancement of information management for the Nuclear Security Enterprise.

Advancing science

The DOE enterprise has a long history of promoting science and has extensive, active research underway in wireless communication activities. Edge devices will interact over 5G networks with one another as well as with intermediate (edge devices on 5G towers) and centralized systems and services, from exascale machines to exabyte data repositories. Beyond fixed infrastructure, scientific facilities such as remote environmental sensor networks will leverage 5G features such as low-power communications to increase the capabilities, scale, and reach made possible with low-cost battery-powered sensors. These advances will open the potential for fundamentally new architectures along the digital continuum, with edge systems preprocessing data in the field and providing near-real-time data forecasts of the movement of a wildfire, hurricane, or toxic plume based on current conditions and updated in near-real time.

Creating new energy jobs

Achieving national objectives for enabling advanced wireless will promote clean energy jobs by harnessing a vast new market, revitalizing the U.S. energy and manufacturing sectors, and creating millions of jobs. Using advanced wireless to achieve DOE's missions could revolutionize how clean energy technologies and products are deployed, potentially creating a new category of clean energy jobs as America transforms its energy sector. There will be an increased need for a vast number of new 5G-enabled sensors and devices, which will create demand for new infrastructure across the country, providing new career paths and retraining opportunities in every type of community nationwide.

Contributions to the Nation

The DOE enterprise's contribution to the national advancement of 5G and beyond capabilities will support the Administration's goals for the United States to be a world-leader in advanced wireless. This is consistent with the *National Strategy to Secure 5G* and the *National Security Strategy*, which calls for investing in and working with a broad range of partners to advance network infrastructure resilience in 5G and other advanced communication technologies.

Advanced wireless can be a catalyst for future discoveries and technologies that have global impacts for a variety of sectors. Ongoing open scientific research can benefit from advancements in many ways including improved throughput with low latency, the ability to deploy more powerful sensors and new sensors

for harsh environments, remote sensing capabilities, microelectronics, and determining implications for other critical infrastructures.

Achieving global leadership in advanced wireless is perhaps one of the biggest critical infrastructure builds of the century and is also central to the United States enhancing the agility and resiliency of the national energy grid. Specifically, it aids in the Department of Homeland Security's National Response Framework Emergency Support Functions (ESF) of Communications (ESF #2), Information and Planning (ESF #5), and Energy (ESF #12). Also, advancing 5G could promote widely available broadband to solve the "last mile" challenge of bringing high speed internet to remote and underserved areas.

Key Challenges

DOE recognizes that advanced wireless is not simply an opportunity, but also presents new and complex challenges as the technology emerges, evolves, and is implemented in more and more contexts. Advanced wireless will create a new threat landscape, and capabilities to detect and mitigate these threats must be developed. The U.S. also remains behind some competitors in the deployment of advanced wireless infrastructure. DOE recognizes that it must harness its scientific expertise to confront the risks and address the technology, security, spectrum, and policy challenges and gaps to leverage the opportunities advanced wireless brings to DOE's mission space.

Spectrum

Legacy approaches to federal spectrum management – allotting slices of frequencies for single-purpose use – continue to support the achievement of the missions of numerous federal agencies, such as the critical DOE missions. This legacy allocation system has also been used to auction off federal spectrum to commercial users. While the commercial sectors demand for federal radio spectrum continues, spectrum is a finite resource, and it is becoming increasingly difficult to identify available spectrum. All of DOE mission requirements must be protected, but the agency must also thoroughly analyze, evaluate, test, train, and potentially incorporate new methods to use available spectrum more efficiently.

The National Telecommunications and Information Administration (NTIA), Federal Communications Commission (FCC), and other federal agencies continue to work collaboratively to support the growing demand for spectrum for both commercial and federal innovation while still protecting federal agency mission requirements. Spectrum regulations, policies, and even technological advances have not kept pace with growing spectrum demands and operational realities. DOE manages over 7500 frequency assignments across the United States, as well as the National Laboratory complex. DOE's spectrum has overlapped frequencies that the NTIA, after appropriate analysis, has requested be made available to the FCC for nonfederal use. DOE has participated in spectrum auctions and continues its work of reallocating its spectrum-dependent systems through funding from the Spectrum Relocation Fund (SRF), including the Advanced Wireless Systems (AWS)-1 and 3 spectrum auctions.

NTIA, through determination by the Policy and Plans Steering Group (PPSG), submits notices requesting quantification analyses of certain bands to determine an agency's feasibility of relocating its spectrum assets. The pace of these requests and scope of analysis have been rapidly increasing. This presents a resource challenge, with some requests taking up to a year to analyze. While initial shared spectrum capabilities, such as Citizens Broadband Radio Service (CBRS), have shown success, the underlying spectrum allocation schemes have been designed more to avoid incumbent interference and assure continuing high operational reliability, rather than for spectral use efficiency. It is therefore vital that DOE establish the capability to study radiofrequency (RF) efficient and effective technologies, as well as to examine all the myriad uses comprising the functionality of these bands to ensure the continued successful execution of ongoing federal and nonfederal critical missions.

Security

Accelerating the development and deployment of 5G and beyond capabilities, while ensuring those systems are robust, protected, resilient, and reliable is a key challenge for the Department and the Nation. Advanced wireless networks transport massive amounts of sensitive data and are therefore particularly attractive targets for potential U.S. adversaries and other malevolent actors. Advanced wireless networks must incorporate suitable protections that address the full range of hardware, software, and human risk factors.

Consistent with Cybersecurity and Infrastructure Security Agency (CISA)[1] findings, DOE must maintain an awareness of and mitigate against the distinct deployment risks introduced by 5G and other advanced wireless applications:

Influencing design and architecture

As organizations and municipalities build out their local 5G networks, they add more Information and Communications Technology (ICT) components to their infrastructure. Many of these components may not have enterprise grade security and come with vulnerabilities that can be readily exploited. More creative threat actors may even attempt to market compromised 5G components with built-in vulnerabilities, hoping to attract unsuspecting organizations with low-cost options for their 5G local network deployment.

Supply chain zero-day attacks

Even if threat actors fail to place vulnerabilities into the ICT components, they may look to infiltrate 5G networks via the supply chain. For example, if a trusted 5G ICT component manufacturer has poor DevOps processes, there is a high likelihood that vulnerabilities may go undetected before commercial release. These potential zero-day vulnerabilities can lead to widespread disruption.

Legacy technologies

5G wireless networks are built on a foundation of legacy technologies, like 4G LTE networks. Therefore, 5G networks are exposed to the same known vulnerabilities from these legacy hardware and software tools. To date, it is not clear how the integration of 5G into the 4G technology stack will impact the new deployment's overarching security posture.

Increased attack surface

Since 5G networks require more components, they increase the number of access points and network edges, ultimately increasing the attack surface. At the very least, the infrastructure likely incorporates cellular towers, radios, baseband units, small cell systems, and mobile devices. These components will increase the digital attack surface, as well as expose the organization to new risks because many of these devices may lack physical security features. For example, a small cell located on an outdoor-facing wall of a building in an urban area may be at increased risk of physical exploitation.

Misconfiguration

Misconfiguration is a perennial challenge for information technology (IT) teams, and it is only going to get harder with the advent of 5G networks. The flexibility in 5G brings with it increased complexity and settings to configure, which also means a higher likelihood of dangerous security configuration flaws. Technologies, controls, and configurations are all modifiable.

1. 5G | CISA

Difficulty updating and repairing custom technologies

To maintain the interoperability necessary to optimize 5G deployments, custom equipment may become a security and availability risk. Customization stymies speed and scale as such equipment may not be easily maintained - making vulnerability management more difficult while also exposing more risks.

Enabling use of cellular devices in secure areas used for protection and control of mission critical and National Security Systems (NSS) supporting DOE's missions remains a key problem. This is true even in unclassified environments hosting NSS in which TEMPEST and other technical security issues associated with the deployment could affect systems in nearby proximity. New 5G technologies such as short-range millimeter wave (mmWave) communications, improved wireless authentication, private enterprise wireless networks, and National Security Agency (NSA) approved encryption are all parts of potential solutions to enabling more effective yet secure work in classified environments. Advanced wireless deployments must meet federal mandates and policies to protect NSS as well as assess and mitigate network threats, e.g., Multi-Access Edge Computing (MEC); core network and slicing; and external threats. To be effective, we also need to ensure proper configuration across platforms and domains. The adoption of Zero Trust Architecture (ZTA) must be considered based on the assumption that any user or device accessing the network is a risk.

Standards

Global

The development of advanced wireless policies and standards serve as the foundation for securing the future communications infrastructure. Those entities that shape the future of these policies and standards position themselves as global leaders and help facilitate secure deployment and commercialization of advanced wireless technologies. The development of technical standards with contributions from adversarial nations has the potential to allow untrusted technologies and equipment to capitalize on standards that are unique to their systems and is indicative of strong influence by such parties among standards bodies, such as the 3rd Generation Partnership Project (3GPP), the leading global telecommunications standards development body for 5G cellular. While 3GPP introduces substantial security improvement to the 5G standards, it also provides operators with flexibility by making some of the security procedures optional. Further, the degree of trust in the underlying hardware and software will also have implications for the security of the systems using them. DOE has not been fully engaged with its interagency partners or international standards organization bodies to ensure that standards development supports both supply chain and network security as well as DOE mission needs.

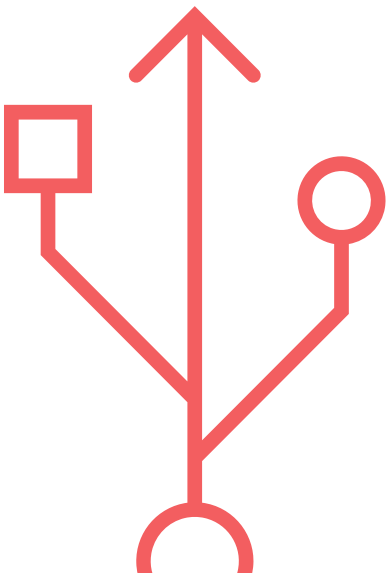
DOE Enterprise

A key challenge across the DOE enterprise associated with adoption of advanced wireless is defining the base use – using public networks or setting up private networks and the pros and cons of both, depending on the situation. There are still gaps in knowledge on how to best use advanced wireless with dynamic controls and configuration for security and resilience within the energy distribution system. Standards are more than just features and must assure us that from supply chain to deployment they represent the appropriate levels of security and technology based on the criticality of our applications to fully enable the mission.

There are also significant issues in working with the mobile service providers while still having autonomy over a network (or a facility). DOE use cases and their requirements have significant differences to those of the commercial ones. Some DOE use cases require much higher uplink bandwidth than the downlink bandwidth which is opposite of commercial use cases. Vendor implemented (or vendor specific) software for the core does not have the tuning knobs to satisfy these requirements. Another issue concerning use of advanced wireless is that many of these services use commercial spectrum. DOE has some difficulty integrating this technology if not using leased service from a commercial provider, and regulatory guidance from the national regulators (NTIA, FCC) has not been forthcoming and is still in the early stages of development.

Investment

Advanced wireless is extremely complex and expensive. Given the DOE's highly federated nature, most advanced wireless activities are limited to single focus areas by specific Departmental Elements or labs. Also, there is no dedicated advanced wireless funding stream or coordination mechanism for collaboration on projects. Current funding opportunities have typically been tied to single labs or discrete projects. There needs to be a concerted effort to not only create a mechanism for collaboration on projects, but also secure new appropriated funds dedicated to new advanced wireless efforts that could bring benefits across the entire enterprise.



Strategic Pillars

DOE will prioritize and invest in the research and development of secure and resilient advanced wireless capabilities. DOE will strive to fulfill this goal through implementation of activities described in the following five strategic pillars: (1) promote advances in spectrum; (2) implement robust security; (3) advance the energy mission; (4) support communications equity; and (5) collaboration. These pillars are not presented in priority order but together represent DOE's near-term priorities for advanced wireless research, development, collaboration, and deployment. The ability to achieve tangible results from the activities described in this strategy will be largely dependent on sufficient funding, resources, and strategic partnerships. Armed with the strategic pillars that follow, DOE is organizing itself and focused on enabling accelerated adoption of advanced wireless to meet its mission needs.

PILLAR 1

Promote Advances in Spectrum

PILLAR 2

Implement Robust Security

PILLAR 3

Advance the Energy Mission

PILLAR 4

Support Communications Equity

PILLAR 5

Collaboration

PILLAR 1

Promote Advances in Spectrum

The transformational uses for advanced wireless capabilities will require operations across all spectrum bands, including the contiguous spectrum available at high frequencies above 24 GHz in the millimeter wave bands. DOE must leverage its expertise to support research, development, testing, acquisition, and fielding of technologies and systems to share this spectrum amongst disparate users, including fostering shared access and capabilities needed for near real-time sharing while preventing harmful interference with incumbent users or legacy systems. As a major user of federal spectrum, DOE must also 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. ***DOE will strive to advance the development of capabilities that secure its access to adequate spectrum through the following:***

A. Define Spectrum Sharing and Dynamic Spectrum Requirements

Invest in activities that promote effective reallocation and sharing of spectrum resources and development of policies and standards that support spectrum sharing and use of dynamic spectrum. Given the finite availability of spectrum and its increased need, spectrum sharing and dynamic spectrum will be key enablers to accomplishing both DOE and national missions. Activities may include execution of a comprehensive dynamic spectrum analysis, engineering study, technology evaluation, and directed research and technology-acceleration efforts to provide definitive data and analysis for spectrum sharing and reallocation policy recommendations, definitive proof-of-concept testing, and technology comparisons. This will enable DOE and other federal agencies to make informed, rapid, and objective decisions on spectrum efficiency and sharing, based upon facts and technical data.

B. Update the 2007 Strategic Spectrum Plan

Update the DOE Strategic Spectrum Plan consistent with the NTIA's approach in developing a National Spectrum Strategy. DOE was responsible for creating and updating a Strategic Spectrum Plan under the Commercial Spectrum Enhancement Act (CSEA) of 2004. That Act was later overturned by the 2010 Presidential Memorandum – Unleashing the Wireless Broadband Revolution. Since then, DOE has relied on NTIA and its development of a National Spectrum Strategy. The DOE Spectrum Working Group is currently updating its plan but will need to ensure that it is consistent with the NTIA strategy currently under

development and includes current technology, policies, processes, and regulations. The update for the DOE Strategic Spectrum Plan for FY 2023 is scheduled to be finalized in October 2022, and the Plan will be updated annually thereafter.

C. Investigate Secure Use of Unlicensed and Shared Spectrum Bands Including Millimeter Wave (mmWave)

Accelerate evaluation of new bands that the FCC is making available for unlicensed and shared use and develop new waveforms that can adapt to the environment. Use of new bands or waveforms for both Wi-Fi and 5G with devices that are now or will be commercially available will make advanced wireless capabilities increasingly available for use by many DOE applications such as smart grid communications. Lower latency, down to 1 ms, will enable massive parallel communications with tens of thousands of local devices. This will be needed for future adoption of more alternative energy sites with many disparate components working in coordination to optimize collection in very dynamic environments.

PILLAR 2

Implement Robust Security

DOE must have a clear and comprehensive understanding of advanced wireless threats and vulnerabilities, including adversaries' capabilities and their intent to leverage advanced wireless technologies against both DOE and U.S. interests. DOE must minimize risks to its advanced wireless infrastructure and supply chains by adhering to stringent monitoring, inspection, physical security, operational security, and to requirements and practices outlined in both Executive Order (EO) 13873, "Securing the Information and Communications Technology and Services Supply Chain," and EO 14028, "Improving the Nation's Cybersecurity." ***DOE will strive to accomplish this through the following:***

A. Develop and Implement Security

Ensure consistent, secure advanced wireless deployments in DOE elements, including the National Laboratories, working in collaboration with each other and with industry to develop security enhancements, protocols, and policies. Key actions should include:

- 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 and demonstrating how such vulnerabilities could be exploited.
    - Researching vulnerabilities in aspects of the ecosystem including but not limited to edge computing, machine learning/artificial intelligence (AI), and all physical layers including the transition between 4G and 5G.
    - Researching and testing to utilize novel features such as network slicing and multi-factor authentication to explore their use for security in both communications and critical infrastructure.
- Ensuring that security measures account for all technologies that would be in the path of the entire network, including the interconnection of devices that may be registered to the advanced wireless network on the edges and not just the internal connection of devices. This should consider all applications, including but not limited to device-to-device internal network communications, communication between on-network devices and external sources such as the cloud, mobile edge computing, and other network slices.
- Providing evidence-based information to regulatory agencies, standards groups, and network operators to inform policy and standards development and decision-making.

B. Implement Supply Chain Risk Management

Continue to emphasize supply chain risk management through testing and vulnerability management programs that address advanced wireless security and vulnerability challenges associated with advanced wireless handsets, radio access networks, and other advanced wireless components. Expanded elements of supply chain risk management may include:

- Sharing best practices and leveraging existing Headquarters or other National Laboratory Supply Chain Risk Management (SCRM) programs, including information on trusted and untrusted vendors, to ensure only trusted vendor products are used in DOE supply chains.
- Establishing an energy sector focused Software Bill of Materials (SBOM) vulnerability identification methodology that provides improved protection of our energy sector 5G communications supply chain.
- Collaborating with Department of Homeland Security (DHS) on Critical Infrastructure Assessments and Analysis teams, including providing National Laboratory experts to current assessment and analysis teams in incident response situations.
- Providing reliable and relevant information to the Electricity Information Sharing and Analysis Center (E-ISAC) on 5G supply chain risks impacting reliable and secure energy production and distribution.
- Using the capability of the National Laboratories to analyze, isolate, verify, and share reliable supply chain vulnerability threat information.
- Expanding the existing national energy infrastructure supply chain knowledge sharing database system to include supply chain risks of 5G components and infrastructure.
- Developing tools that characterize network behavior to ensure proper operation and identify new supply chain vulnerabilities.

C. Enhance Monitoring

Increase and enhance the ways in which DOE monitors for threats targeting its mission space with a particular focus on securing the internet-connected and virtual private wireless networks utilized by the PMAs to enhance grid security and reviewing and updating monitoring and data analytics requirements and capabilities to detect any threats to the advanced wireless networks. Other monitoring activities may include:

- Monitor Energy Control 5G Communications Networks: Cooperate with the National Laboratories, North American Energy Reliability Model, the National Grid Modernization Program, and the E-ISAC to monitor evolving 5G threats, analyze what impact these evolving threats have on our national energy systems, and provide proactive information enabling energy operators to take corrective measures prior to any 5G-based cyber-attack.
- Monitor Environmental Impacts: Create research programs, engineering guides, sensor layouts, data collection, and curation to enable environmental monitoring. Low latency flow access to high performance computing in the field will assist environmental monitoring by turning collected data into an automated response that can detect and prevent events such as wild-fires, understand sub-surface events, as well as direct high-cost sensors to focus on the right spot to capture once in a life-

time events necessary to advance science. This will also help achieve Pillar 3, Advance the Energy Mission.

- Monitor Critical Transportation and Asset Location Security: Establish programs to research, develop, employ, monitor, and create long term tracking capabilities to improve shipping and asset security for critical energy assets. Critical energy assets, particularly atomic and special nuclear materials, have stringent condition, logistic, and accountability requirements and are frequently stored for long periods of time. New 5G Internet of Things (IoT) devices developed by commercial entities and National Laboratories will enable more efficient shipping and tracking mechanisms, critical machinery monitoring, even future harsh environment monitoring such as jet turbines, engines, and furnaces for electricity production or high temperature manufacturing.

D. Deploy Classified 5G and Beyond

Facilitate the digitization, automation, and connectivity to machines and transport solutions through classified 5G. To maintain the confidentiality (protection of data in transit, at rest, and in use), integrity (protection against changes in data), and availability (protection against network interruption) of both classified and unclassified 5G networks, DOE must look toward mandates, necessary policy updates, and requirements for its deployment. In the meantime, DOE will focus on the protections around 5G for different classification levels and adopt Zero Trust (ZT) principles that call for explicit verification, "least privilege," and assumes breach. Using the ZT approach, DOE will work to deploy technologies for secure operations through insecure networks. This will provide the availability, confidentiality, and integrity of data that is needed for DOE operations. As we implement the ZT model, DOE will investigate the role of AI and machine learning in mitigating security risks, defining expected behavioral patterns, and identifying abnormalities. Data analytics will provide insight into network automation and orchestration given the large amount of data that will traverse 5G networks.

E. Evaluate Open Architectures including Open Radio Access Network (ORAN)

Contribute to the development of advanced wireless network architectures that inform more-secure designs for both core and edge systems, including ORAN and network slicing. This includes working with industry and conducting research and development to promote open interfaces in both the RAN and 5G Core that allow for more competition and innovation, and more robust security.

- ORAN Acceleration Program: Provide a capability to enable multiple developmental vendors to test, evaluate, and showcase ORAN component improvements in an unbiased and collaborative realistic, full-scale setting. This will be particularly beneficial to smaller, disadvantaged developers to help them get access to major market 5G ORAN adopters. This will further DOE's collaboration with NTIA, the Department of Defense, and other federal agencies as well as global 5G adopters, and developers to analyze ORAN security vulnerabilities and provide input for development of reliable security standards and analysis accelerating development of ORAN commercial solutions.
- To the extent possible, and consistent with security and mission requirements, ensure that DOE's own developmental designs and procurements are compatible with open standards.

PILLAR 3

Advance the Energy Mission

Advanced wireless supports DOE cutting-edge research that will enable grid transformation with ultra-reliable, low-latency communications for smart grid automation at much higher densities and scales; secure bi-directional sharing of selected edge information for transactions between various smart grid stakeholders and novel applications of 5G for smart grids such as self-interconnection and context-based security. In addition to grid transformation, ***DOE will strive to utilize this technology to further its energy missions and secure the path to Net Zero through the following:***

A. Secure the Path to Net Zero: National Energy Grid Security Test Platform

Invest in development of a national energy grid security test platform. Such a platform would provide and facilitate open access for energy grid modernization technologies and advanced wireless secure and reliable communications interconnections. This would be accomplished through a research and testing environment for interaction with other test beds and the incoming flexible nuclear power generating technologies like microreactors to interact at the convergence of control, cybersecurity, resiliency, and reliability. Such a platform, coupled with Human-in-the-Loop (HIL) simulation and modeling capabilities both for power and communications, will link simulation and modeling with deployed field equipment at scale.

B. Invest in Grid Modernization

Continue to invest in research and development on how secure, advanced wireless can be used to improve the nation's electrical grid infrastructure, making it more flexible, reliable, resilient, secure, and sustainable. Such activities may include:

- Developing the technologies and tools to enable the integration of renewable energy resources on electric power systems.
- Developing techniques and tools to measure weather resources and power systems, forecast renewable resources and grid conditions, and convert measurements into operational intelligence to support grid operations and planning.
- Developing methods for real-time operation and control of power systems at various scales to support a more reliable and efficient electric grid.
- Developing tools, algorithms, and methods for modeling, simulating, and designing the electric power system at all scales.

C. Support the Science

Continue to invest in the advancement of science and development and use of 5G related capabilities. Related areas of research important to advancing 5G and beyond to support DOE's science-based research include:

- Multi-Access Edge Compute (MEC). Develop a robust ability to securely automate, deploy, and manage compute resources at non-traditional locations within the scientific network, including within wireless components of that network. The integration of sensors with HPC resources will be a powerful tool for climate, energy, and high energy physics applications, among others. This will depend on being able to not just move data efficiently and securely but also to effectively process and analyze data before its moved to a data center.
- New Materials. Examine the use of 5G for science including device and materials design realms. Scientific requirements for 5G and beyond significantly exceed those of commercial telecommunications applications. Edge devices, including sensors, edge computers, and radios, will have to operate in extreme environments with inordinate, rapid changes in temperature, high pressure, or exposure to water or corrosive materials.

D. Evaluate Secure Distributed Energy Control and Communication

Conduct research into the most effective, secure, and resilient ways to apply 5G to future generations of critical energy production systems. These systems all share the requirement to have resilient, robust, efficient, and secure communications systems. 5G and 6G framework systems are likely candidates for part of the development of these essential energy production systems, but such use cases require significant research and engineering.

PILLAR 4

Support Communications Equity

Rural and underserved communities often do not have access to wireless broadband (or broadband at all) but have energy distribution connectivity that could be leveraged to provide wireless solutions for these local communities. Therefore, ***DOE will strive to use its assets to promote deployment of broadband capability to rural and underserved communities.***

A. Support Implementation of the Infrastructure Investment and Jobs Act (IIJA)

Continue to work with state, local, tribal, and territorial (SLTT) partners as well as the interagency on how to support implementation of the IIJA, which sets forth a $65 billion investment into broadband. However, most of those funds are being administered by NTIA, and there are statutory requirements for the funds to be distributed to state and local governments as opposed to federal departments and agencies. Therefore, in addition to offering support where practical to specific IIJA projects, DOE will embark on its own efforts to support digital inclusion and diminish the digital divide. Such efforts may include:

- Developing a program to engage and assist energy transmission and distribution agencies to develop, engineer, and evaluate wireless broadband (5G) solutions. Such a program would establish 5G core assessment capability, promote partnerships between energy providers and commercial communications providers, and create an academic grants program to study 5G and beyond security and network stability for rural and underserved areas. This DOE capability would support policy optimization, technical support, engineering, and evaluation assistance to bridge the digital divide and empower energy providers to accelerate wireless broadband to rural and underserved communities.
- Engaging with SLTT entities to optimize delivery of high-speed backbone and wireless broadband capability through use of the national energy right of way and power infrastructure.
- Providing grants and engineering assistance to encourage and help coordinate public and private energy providers to assist deployment of broadband capabilities to rural and underserved communities.

PILLAR 5

Collaboration

Ensuring that the DOE enterprise is seen as a key leader for research, development, delivery, and application of advanced wireless requires visibility, transparency, and collaboration and will be critical to the success of this strategy. To be successful, the Department must understand the full breadth of its current work, leverage its technologies and best practices, and share discoveries and lessons learned with partners. DOE must lend its expertise and work collaboratively with industry, the interagency, and international bodies to influence standards to meet DOE and national needs. ***DOE will strive to accomplish this through the following:***

A. Establish a Standing Information Sharing Body

Transform the current informal 5G working group into a standing venue to share best practices, lessons learned, readouts of important meetings or interactions, new research, use cases, and testing initiatives. The group will be led by the Office of the Chief Information Officer (OCIO) and its purpose will be to coordinate communication across stakeholders. The group will leverage both technology diversity and commonality to maximize visibility across the enterprise and provide a venue for development of cross laboratory / cross disciplinary research opportunities to meet DOE mission needs.

B. Establish Integrated Product Teams

Develop advanced wireless integrated project teams to drive uses cases and create cross laboratory/cross disciplinary opportunities to build DOE capabilities in the 5G/advanced wireless space. To be successful, DOE will need to leverage all available technical expertise across its enterprise. For example, a lab with the necessary field-programmable gate array (FPGA) experience may not have the right antenna resources, while a third lab has the necessary expertise in custom semiconductor and materials fabrication. These teams could also collaborate with the mobile service providers and key industrial partners to further the ability to do applicable research.

C. Evaluate Interoperability Solutions

Study the feasibility of interconnecting diverse experimental grid technologies between laboratory testbeds and general interoperability between National Laboratory wireless testbeds. In most cases, laboratory advanced wireless efforts are in partnership with, or resident upon, commercial networks. In some cases,

other technologies such as stand-alone networks or CBRS are being employed by DOE sites. As part of Integrated Research Initiative efforts, or in support of efficient interoperability, it is important to ensure that these efforts a) know about each other, b) can and are encouraged to collaborate, and c) identify research opportunities created to explore how these wireless testbeds can be integrated from the standpoint of device roaming, data backhaul, and streamlining spectrum availability based on a common understanding of standards and practices.

D. Enhance Public-Private Partnership

Expand outreach to private sector partners working on broad, 5G structural challenges that are of mutual interest and benefit to both communities. The private sector is making rapid advances in applied 5G platforms that have application for DOE mission sets, including frequency usage optimization, emergency first responder to national site collaboration, advanced manufacturing, right of way and backbone support to rural and underserved communities, and wireless critical systems control through ultra-low latency high reliability communications. OCIO and the DOE enterprise, especially the National Laboratories, are or already have developed a unique set of tools for working through 5G challenges, including building test beds for optimizing spectrum usage, enhanced security, effective public-private broadband coverage, emergency first response and disaster recovery, and improved resilience for high criticality systems. Exchanging information on broader challenges and means for reducing risk in development will advance rapid employment of 5G tools across both sectors.

E. Support Work of Standards Setting Bodies

More fully lend technical expertise and engage the interagency to ensure appropriate representation within bodies such as 3GPP, the Alliance for Telecommunications Industry Solutions (ATIS), and O-RAN Alliance. This will ensure U.S. participation in such organizations seeks outcomes that meet DOE mission needs and promote security, interoperability, and resilience.

F. Promote the Strategic Partnership

Continue to advertise and support Strategic Partnership Projects (SPP) with the interagency and international partners to enable the National Laboratories to work with external sponsors who provide mission space and funding for specific projects. This will lead to exciting new innovations that can be leveraged to accelerate DOE and national efforts to achieve advanced wireless goals.

G. Conduct International Outreach

Continue to conduct regular consultations with key international partners on a range of advanced wireless issues. International cooperation provides the opportunity to share best practices, lessons learned, and leverage technology developments with key allies and partners. OCIO currently has close bilateral relationships with the UK, Germany, Israel, and Poland, and is seeking to expand to other willing and like-minded nations. International efforts will include coordinating visits by international partners to National

Laboratories of interest; involving lab experts in key interagency discussions with international delegations as appropriate (e.g., Quad Critical and Emerging Technology efforts); providing training to international partners, such as through Cyber Fire; and supporting and promoting the SPP.

Conclusion

The transition to 5G and beyond presents a wealth of opportunities and new capabilities, changing the way the world operates. This transformative technology will enable DOE missions from grid modernization and renewable energy to advances in security applications. DOE will continue working across the enterprise and with key interagency and international partners to share best practices and information related to developments in advanced wireless to leverage efficiencies and further enable its application and deployment. DOE, including the OCIO, will require significant new and sustained investment, research, development, and deployment efforts to implement the key pillars identified in this strategy and to realize the significant benefits advanced wireless can bring not only to DOE missions, but also the Nation.