National Strategy to Secure 5G Implementation Plan
January 6, 2021

Introduction

Activity 0.1: Description of United States interests
Activity 0.2: Departments and agencies roles and responsibilities

Line of Effort One: Facilitate Domestic 5G Rollout

Activity 1.1: Research, Development, & Training to reach and maintain United States leadership in 5G and beyond
Activity 1.2: Identify incentives and options to leverage trusted international and domestic partner suppliers

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure

Activity 2.1: Risk evaluation of domestic and international suppliers
Activity 2.2: Assess threats, vulnerabilities, and risks to 5G Infrastructure
Activity 2.3: Identify security gaps and threats to United States and strategic partners' supply chains
Activity 2.4: Assessment of global competitiveness and (economic) vulnerabilities of United States manufacturers / suppliers
Activity 2.5: Identify/develop/apply security principles for 5G infrastructure in the United States

Line of Effort Three: Address Risks to United States Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide

Activity 3.1: Identify incentives and policies to close security gaps
Activity 3.2: Identify incentives and policies to ensure United States industrial base economic viability
Activity 3.3: Address the risk of 'High-Risk' vendors in United States 5G infrastructure (forward looking)
Activity 3.4: Private sector engagement on 5G security
Activity 3.5: Establish acquisition processes to facilitate 5G infrastructure for classified information requirements.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G

Activity 4.1: Diplomatic Engagement for Risk Mitigation, Standards, and Security Principles
Activity 4.2: Provide Technical Assistance to International Partners
Activity 4.3: Options for mitigating security risk from untrusted equipment in international partners systems
Activity 4.4: Promote United States leadership in international standards development for 5G, including through private sector and international engagement
Activity 4.5: Joint testing environments with international partners
Activity 4.6: Policies and strategies for global market competitiveness and diversity of secure 5G infrastructure

Annexes

A. Plan for Research, Development, & Testing
B. Plan for Diplomatic Engagement
C. Plan for Technical Assistance to International Partners
D. Plan to Promote United States Leadership in International Standards Development for 5G
E. Strategic Framework for Global Market Competitiveness and Diversity of Secure 5G Infrastructure
F. Summary of Potential Legislative Requirements

Appendices

1. Information And Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force (TF) Threat Evaluation Working Group: Threat Scenarios, CISA, February 2020
2. CISA 5G RDT&E Efforts Infographic, CISA, May 2020
3. Overview Of Risks Introduced By 5G Adoption In The United States, CISA, July 31, 2019
4. Executive Order 13873 Response - Methodology For Assessing The Most Critical Information And Communications Technologies And Services, CISA, April 2020
5. Summary of Responses to the NTIA Secure 5G Request for Comment, National Telecommunications and Information Administration, July 27, 2019

Executive Summary

As stated by President Trump in the March 2020 National Strategy to Secure 5G, "Fifth generation wireless technology, or 5G, will be a primary driver of our Nation's prosperity and security in the 21st century". The National Strategy to Secure 5G details how the United States along with like-minded countries will lead global development, deployment, and management of secure and reliable 5G infrastructure. The work to enhance the security of 5G networks will require a range of efforts from across the United States Government, working in close collaboration with our international and industry partners. The United States Government is committed to fostering innovation and realizing the technological promise of 5G, while continuing to safeguard our economy and national security and ensuring continued access to 5G networks, with lawful authorization, for critical government functions.

In accordance with the Secure 5G and Beyond Act of 2020, the Executive Branch has developed a comprehensive implementation plan. This implementation will be managed under the leadership of the National Security Council and the National Economic Council, supported by the National Telecommunications and Information Administration (NTIA), and with contributions from and coordination among a wide range of departments and agencies. The implementation plan took into account the 69 substantive comments in response to NTIA's Request for Comments received from companies, industry associations, and think tanks representing a range of interests and aspects of the telecommunications ecosystem. Consistent with the National Strategy to Secure 5G, the implementation plan encompasses four lines of effort, which are detailed below.

Line of Effort One: Facilitate Domestic 5G Rollout

The first line of effort establishes a new research and development initiative to develop advanced communications and networking capabilities to achieve security, resilience, safety, privacy, and coverage of 5G and beyond at an affordable cost. Advancement of United States leadership in Secure 5G and beyond systems and applications will be accomplished by enhancing centers of research and development and manufacturing. These efforts will leverage public-private partnerships spanning government, industry, academia, national laboratories, and international allies. This line of effort also intends to identify incentives and options to leverage trusted international suppliers[1], both to facilitate secure and competitive 5G buildouts, and to ensure the global competitiveness of United States manufacturers and suppliers.

Line of Effort Two: Assess Risks to & Identify Core Security Principles of 5G Infrastructure

[1] For the purposes of this implementation plan, determination of whether a supplier is "trusted" is intended to occur via rigorous supplier evaluation, as noted in the "Prague Proposals," which take into account the rule of law; the security environment; ethical supplier practices; and a supplier's compliance with secure standards and industry best practices. Specifically, evaluations should include the following elements: (1) Whether network hardware and software suppliers are subject, without independent judicial review, to control by a foreign government; (2) Whether network hardware and software suppliers are financed openly and transparently using standard best practices in procurement, investment, and contracting; (3) Whether network hardware and software suppliers have transparent ownership, partnerships, and corporate governance structures; and (4) Whether network hardware and software suppliers exemplify a commitment to innovation and respect for intellectual property rights. These criteria are intended to be complimentary to and used alongside the additional trust principles developed via Activity 2.1, and additional security principles developed via Activity 2.5 of this implementation plan.

The second line of effort is oriented toward identifying and assessing risks and vulnerabilities to 5G infrastructure, building on existing capabilities in assessing and managing supply chain risk. This work will also involve the development of criteria for trusted suppliers and the application of a vendor supply chain risk management template to enable security-conscious acquisition decision-making. Several agencies have responsibilities for assessing threats as the United States' manages risks associated with the global and regional adoption of 5G network technology as well as developing mitigation strategies to combat any identified threats. These threat assessments take into account, as appropriate, requirements from entities such as the Committee on Foreign Investment in the United States (CFIUS), the Executive Order (E.O.) on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom), and the Federal Acquisition Security Council (FASC). In addition, this line of effort will identify security gaps in United States and international supply chains and an assessment of the global competitiveness and economic vulnerabilities of United States manufacturers and suppliers. Finally, this set of activities will include working closely with the private sector and other stakeholders to identify, develop, and apply core security principles for 5G infrastructure. These efforts will include leveraging the Enduring Security Framework (ESF), a working group under the Critical Infrastructure Partnership Advisory Council (CIPAC). These emerging security principles will be synchronized with or complementary to other 5G security principles, such as the "Prague Proposals" from the Prague 5G Security Conference held in May 2019.

Line of Effort Three: Address Risks to United States Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide

The third line of effort involves addressing the risks to United States economic and national security during the development and deployment of 5G infrastructure worldwide. As a part of this effort, the United States will identify the incentives and policies necessary to close identified security gaps in close coordination with the private sector and through the continuous evaluation of commercial, security, and technological developments in 5G networks. A related activity is the identification of policies that can ensure the economic viability of the United States domestic industrial base, in coordination with the private sector through listening sessions and reviews of best practices. An equally important activity relates to the identification and assessment of "high risk" vendors in United States 5G infrastructure, through efforts such as the Implementation of E.O. 13873, on "Securing the Information and Communications Technology and Services Supply Chain." These efforts will build on the work of the CFIUS, the FASC, and Team Telecom reviews of certain Federal Communications Commission (FCC) licenses involving foreign ownership. This element of the implementation plan will also involve more intense engagement with the owners and operators of private sector communications infrastructure, systems equipment developers, and other critical infrastructure owners and operators. The engagements will involve sharing information on 5G and future generation wireless communications systems and infrastructure equipment. Such work will be conducted through the Network Security Information Exchange, the IT and Communications Sector and Government Coordinating Councils, the National Security Telecommunications Advisory Committee, and NTIA's Communications Supply Chain Risk Information Partnership (C-SCRIP).

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G

The fourth line of effort addresses the responsible global development and deployment of 5G technology. A key component of this line of effort is diplomatic outreach and engagement to advocate for the adoption and implementation of 5G security measures that prohibit the use of untrusted vendors in all parts of 5G networks. A related component involves the provision of technical assistance to mutual defense treaty allies and strategic partners of the United States to maximize the security of their 5G and future generations of wireless communications systems and infrastructure. The goal of providing financing support and technical assistance is to help enable countries and private companies to develop secure and trusted next generation networks that are free of untrusted vendors and that increase global connectivity. A key part of 5G deployment involves international standards development, thus the implementation plan outlines several steps in support of the goal of strengthening and expanding United States leadership in international standards bodies and voluntary consensus-based standards organizations, including strengthening coordination with and among the private sector. This line of effort will also include collaboration with allies and partners with regard to testing programs to ensure secure 5G and future wireless communications systems and infrastructure equipment, including spectrum-related testing. To successfully execute this work, continued close coordination between the United States Government, private sector, academic, and international government partners is required to ensure adoption of policies, standards, guidelines, and procurement strategies that reinforce 5G vendor diversity and foster market competition. The overarching goals of this line of effort are to promote United States-led or linked technology solutions in the global market; remove and reduce regulatory and trade barriers that harm United States competitiveness; provide support for trusted vendors; and advocate for policies and laws that promote open, competitive markets for United States technology companies. This will also be supported through close collaboration with partners on options to advance the development and deployment of open interfaced, standards-based, and interoperable 5G networks.

Introduction

Activity 0.1. Description of United States Security Interests. This section includes a description of United States national and economic security interests pertaining to the deployment of 5th and future generations wireless communications systems and infrastructure.

As stated in the National Strategy to Secure 5G, Fifth Generation wireless technology, or 5G, will be a primary driver of our Nation's prosperity and security in the 21st century. 5G will provide orders of magnitude improvements in multiple areas, including speed, connectivity, and reduced latency. As a result, this new technology will provide consumers, businesses, and governments with remarkably fast network connections that will enable tens of billions of new devices to harness the power of the Internet, transforming the way we live, work, learn, and communicate.

This technology will spur innovation and enable the development of new markets, products, services, and economic growth around the world. These new connections will empower a vast array of new and enhanced critical services, from autonomous vehicles and tele-medicine, to helping communities enhance the management of local resources such as traffic signals and water supplies, to automated manufacturing and advances to traditional critical infrastructure, such as smart grid electricity distribution. Consumer devices from vehicles to medical implants will become more capable via 5G connections to new edge computing and cloud services, algorithms, and applications. 5G deployment will bring a new generation of the knowledge economy; increasing productivity, growing new businesses, and spurring innovation. Given 5G's scope touching virtually everything in our daily lives the stakes for safeguarding these vital networks and architecture could not be higher.

The security of 5G information and communications technology and services (ICTS) infrastructure, and the data and information that transits and is stored on it, is a key United States security interest. A trusted, secure supply chain is also paramount. We cannot ensure the security of 5G networks if untrusted equipment or software is allowed to control any part of the network, including the radio access network (RAN).

It is a key interest of the United States to address unacceptable risks that come from ICTS products designed, developed, manufactured or supplied by companies operating under the control or influence of a foreign government whose national security interests are adverse to the United States.
Lead Entity: National Economic Council and National Security Council

Activity 0.2. Department and agency roles and responsibilities. This section provides a description of the roles and responsibilities of the appropriate executive branch agencies and departments and agencies mechanisms to coordinate implementation of the Strategy.

President Trump has set American leadership in 5G as one of the major priorities of this Administration. As he previously noted, "[s]ecure 5G networks will absolutely be a vital link to America's prosperity and national security in the 21st century… [w]e cannot allow any other country to out-compete the United States in this powerful industry of the future."

The Administration's multifaceted efforts on 5G are led by the Assistant to the President and Director of the National Economic Council (NEC), in close coordination with the Assistant to the President and

National Security Advisor at the National Security Council (NSC). This integration between the NEC and NSC is ensures the United States Government is leveraging strong expertise in national security and economic disciplines for the United States leadership in 5G.

Through a regular 5G department and agency coordination process, the NEC and NSC are working together to lead and coordinate the activities of more than 15 departments and agencies, including efforts to set core security principles and accurately identify cybersecurity risks; address those risks through initiatives to secure the ICTS supply chain; facilitate increased engagement in technical standards-setting organizations by private and public sector stakeholders; support rapid domestic deployment of 5G services by ensuring the availability of appropriate spectrum and a conducive regulatory environment; and engage at the international level to promote security in all aspects of 5G networks worldwide.

Such a vital, yet complex, initiative requires a unified governmental approach, and this effort has benefitted tremendously from integrating the unique perspectives and expertise of NEC, NSC, and departments and agencies. We are confident that going forward, our collaborative management of government-wide 5G efforts creates an environment in which every available resource can be most effectively brought to bear as we rise to the challenge of assuring American leadership in 5G and the generations of communications technologies to come.

Departments, agencies, and other Federal entities participating in this implementation plan include:

Department of Commerce (DOC)
- Bureau of Economic Analysis (BEA)
- Bureau of Industry and Security (BIS)
- International Trade Administration (ITA)
- National Institute of Standards and Technology (NIST)
- National Telecommunications and Information Administration (NTIA)
- United States Patent and Trademark Office (USPTO)

Department of Defense (DOD)
- Defense Advanced Research Projects Agency (DARPA)
- National Security Agency (NSA)

Department of Education (ED)
Department of Energy (DOE)
Department of Homeland Security (DHS)
- Cybersecurity and Infrastructure Security Agency (CISA)

Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)

Department of Labor (DOL)
Department of State
Department of Transportation (DOT)

Executive Office of the President (EOP)
- National Economic Council (NEC)
- National Security Council (NSC)
- Office of Management and Budget (OMB)
  - Federal Chief Information Council Federal Mobility Group (FMG)
- Office of Science and Technology Policy (OSTP)
  - National Science and Technology Council (NSTC)
    - Networking and Information Technology Research and Development (NITRD) Program
- Office of the United States Trade Representative (USTR)

Federal Communications Commission (FCC)
Food and Drug Administration (FDA)
General Services Administration (GSA)
National Science Foundation (NSF)
Office of the Director of National Intelligence (ODNI)
Small Business Administration (SBA)
The Export-Import Bank of the United States (EXIM)
United States Agency for International Development (USAID)
United States International Development Finance Corporation (DFC)
United States Trade and Development Agency (USTDA)

Lead Entities: National Economic Council (NEC) and National Security Council (NSC)

Line of Effort One: Facilitate Domestic 5G Rollout

The Administration is facilitating the private sector-led domestic rollout of 5G, primarily coordinated by the National Economic Council.

Activity 1.1: Research, development, and testing to reach and maintain United States leadership in secure 5G and beyond[2].

This activity outlines the approach for research and development (R&D) by the Federal Government, in close partnership with trusted supplier entities, mutual defense treaty allies, academia, strategic partners, and other countries to reach and maintain United States leadership in 5th and future generations wireless communications systems and infrastructure security. A detailed plan is provided in Annex A.

The objectives for the R&D approach include:

1. Develop the advanced communications and networking capabilities necessary to achieve the security, resilience, safety, privacy, capacity, coverage, and performance of 5G and beyond systems at an affordable cost;
2. Enable the establishment and enforcement of a trusted end-to-end hardware, software, and network management ecosystem to reduce, manage, and mitigate security vulnerabilities;
3. Advance technical standards, strong intellectual property rights (IPR), and educational and workforce opportunities in 5G and beyond;
4. Establish a stable and thriving United States manufacturing base for 5G and beyond systems, and create public-private partnerships with government, industry, and academia; and
5. Maximize the strategic effect of Federal R&D resources through an understanding of market needs and by complementing United States private sector activities.

Lead Entity: OSTP

Supporting Entities: DARPA, DHS, DOD, DOE, DOL, DOT, State, ED, FBI, FCC, FDA, FMG, NIST, NSA, NSF, and NTIA.

Outcome Statement: The goal of this activity is to advance and sustain United States leadership and the state of the art in secure 5G and beyond systems and applications by (1) catalyzing the transition of 5G and beyond systems to a secure, open ecosystem of innovators, suppliers, and operators; (2) creating new as well as enhancing existing centers of domestic 5G and beyond research, development, manufacturing, and operations built on United States technological strengths; and, (3) leveraging public-private partnerships spanning government, industry, academia, national laboratories, and international allies. This plan seeks to build and maintain secure, high-performance 5G and beyond systems through synergistic efforts in research, development, and testing.

See Annex A - Plan for Research, Development, & Testing.

[2] *Approval of the plan will not guarantee that resources will be provided for the activity. Departments and agencies will be expected to request resources for the R&D actions and activities through their established budget process unless the activity describes an alternative means for acquiring the resources.*

Activity 1.2: Identify incentives and options to leverage trusted international partner and domestic suppliers.

This activity seeks to provide identification of incentives and policy options for leveraging the communications equipment suppliers from mutual defense treaty allies, strategic partners, and other countries to ensure that private industry in the United States has adequate sources for secure, effective, and reliable 5th and future generations wireless communications systems and infrastructure equipment.

The United States government is taking a multi-pronged approach to ensure the nation's global leadership in 5G as well as its security. This approach includes diplomatic engagements as well as executive actions, and public/private engagement to support industry-driven efforts. While these actions seek to secure the nation's critical communications infrastructure for our future, a critical challenge for the United States and its telecommunications providers is how to continue to incentivize secure and competitive 5G buildouts, and to ensure the global competitiveness of United States manufacturers/suppliers.

Over the last 3 decades, the telecommunications network equipment market has experienced consolidation with the five major suppliers of Radio Access Network (RAN) equipment to be Huawei, Ericsson, Nokia, Samsung, and ZTE. Huawei and ZTE are Chinese companies that the United States has deemed untrustworthy and given these concerns, the Cybersecurity and Infrastructure Security Agency (CISA) conducted an economic analysis of the 5G RAN market that assessed whether certain policy proposals related to 5G (e.g., rip and replace, the establishment of a fund to support supply chain innovation, and the harmonization of new spectrum allocations for 5G with global ones) would support trusted RAN suppliers, support new entrants, and curtail the growth of untrusted suppliers. Based on its analysis, CISA assessed that establishing R&D grants to support supply chain innovation would advance all three strategies, but further analysis is necessary to determine which policy options would be the most effective in terms of ensuring an adequate supply of trusted RAN equipment to meet United States demand.

Lead Entity: DOC/NTIA

Supporting Entities: DHS, CISA, State, DOD and OSTP

Outcome Statement: The United States Government will develop and summarize possible incentives and policy options for leveraging the communications equipment suppliers from mutual defense treaty allies, strategic, other partner nations, as well as domestic suppliers to accelerate 5g rollout in the United States.

Line of Effort Two: Assess Risks to and Identify Core Security Principles of 5G Infrastructure

The Administration will promote secure and reliable 5G infrastructure by regularly assessing the economic and national security and other risks to this infrastructure and defining and maintaining the relevant core security principles for this infrastructure.

Activity 2.1: Risk evaluation of domestic and international suppliers.

This activity provides 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 beyond technology and infrastructure.

Lead Entity: CISA

Supporting Entities: DHS, State, DOC, DOD, FCC, and ODNI-directed agencies.

Outcome Statement: The United States Government will be informed by and make risk-based strategic decisions based on the evaluation of available domestic and international 5G suppliers.

Activity 2.2: Assess threats, vulnerabilities, and risks to 5G infrastructure and supply chain.

This activity provides identification and assessment of potential security threats and vulnerabilities to the infrastructure, equipment, systems, software, and virtualized networks that support 5th and future generations wireless communications systems, infrastructure, and enabling technologies. Assessments shall, as practicable, include a comprehensive evaluation of the full range of threats to, and unique security challenges posed by, 5th and future generations wireless communications systems and infrastructure, as well as steps that public and private sector entities can take to mitigate those threats. This activity also proposes the development of an ongoing capability to identify security vulnerabilities in 5th and future generations wireless communications systems.

Lead Entity: CISA

Supporting Entities: DHS, ODNI, FCC, DOT, and ODNI-directed agencies

Outcome Statement: The Nation has an informed understanding of the threats, vulnerabilities, and risks to operating within a 5G environment, enabling risk-informed decisions regarding 5G technologies and infrastructure.

Activity 2.3: Identify security gaps and threats to United States and strategic partners' supply chains.

This activity seeks to identify where threats and security gaps exist in the United States domestic or mutual defense treaty allies and strategic partners communications equipment supply chain for 5th and future generations wireless communications systems and infrastructure. See Activity 3.1 for the incentives and policy options identified to close gaps identified under this activity.

Lead Entity: ODNI

Supporting Entities: CISA, DHS, OSTP, DOD, DOC/NIST, State, FCC, and ODNI-directed agencies.

Outcome Statement: A department and agency assessment of the threat of foreign adversaries exploiting vulnerabilities in ICTS supply chains stemming from the foreign design, development, manufacture, or supply of United States domestic and strategic partners' communications equipment and infrastructure, or by foreign adversaries conducting supply chain operations against trusted supply chains.

Activity 2.4: Assessment of global competitiveness and (economic) vulnerabilities of United States manufacturers / suppliers.

This activity provides identification and assessment of the global competitiveness and vulnerabilities of United States manufacturers and suppliers of 5th and future generations wireless communications equipment.

Lead Entity: DHS

Supporting Entities: CISA, FCC, DOC, and GSA

Outcome Statement: The United States Government attains an informed understanding of the global competitiveness and economic vulnerabilities of United States 5G manufacturers and suppliers.

Activity 2.5: Identify/develop/apply security principles for 5G infrastructure in the United States.

This activity outlines how the United States Government will work with the private sector to identify, develop, and apply core security principles - best practices in cybersecurity, supply chain risk management, open and interoperable network architecture, and public safety - to United States 5G infrastructure. The principles will be synchronized with other appropriate security principles such as the "Prague Proposals" from the Prague 5G Security Conference in May 2019, and informed by inputs provided through public comment in Appendix 5. Partner with United States industry on principles to promote the transition towards open and interoperable network deployment through rapid innovation and collaboration in the 5G marketplace. (Aligns with Activity 4.2)

Lead Entity: DHS

Supporting Entities: CISA, NSA, DOD, DOJ, FCC, DOC/NTIA

Outcome Statement: The United States Government will provide an action plan for identifying and developing principles (engagements, partner/stakeholder participation) as well as for the application of principles.

Line of Effort Three: Address Risks to United States Economic and National Security during Development and Deployment of 5G Infrastructure Worldwide.

The United States Government will address the risks presented by the use of 5G to its economic and national security by analyzing the risks of 5G infrastructure and ensuring national critical functions and national essential functions are structured in such a way that they are resilient to these risks.

Activity 3.1: Identify incentives and policies to close security gaps.

This activity outlines an approach for the (a) identification of incentives and policy options to help close or narrow any security gaps identified under activity 2.2 and 2.3, and (b) ensure the economic viability of the United States domestic industrial base, including research and development in critical technologies and workforce development in 5th and future generations wireless communications systems and infrastructure.

Many of the activities outlined in the National Strategy to Secure 5G, and in this implementation plan, help to directly and indirectly close security gaps in National telecommunications infrastructure and 5G networks. The FCC, through its Public Safety and Homeland Security Bureau, recently issued orders designating Huawei and ZTE as national security threats and thus banning recipients of federal Universal Service Fund support from using that federal support on equipment or services from these suppliers. Additionally, the Executive Branch has taken numerous actions, such as issuing E.O. 13873, and placing Huawei on the Department of Commerce Entity List, which will further reduce and prevent security gaps as they are fully implemented. Complementary to these actions, the Congress should consider funding the Secure and Trusted Communications Networks Reimbursement Program authorized in section four of the Secure and Trusted Communications Networks Act of 2019, which would facilitate the removal of untrusted equipment and services from our Nation's telecom networks.

Lead Entity: EOP/NEC

Supporting Entities: DHS, OSTP, DOC/NTIA, DOJ, and FCC

Outcome Statement: The United States Government develops options for incentives and policies to close security gaps. Development of options will include engagement with international partners, the private sector, and continuous evaluation of commercial, security, and technological developments in 5G networks.

Activity 3.2: Identify incentives and policies to ensure United States industrial base economic viability.

This activity is intended to ensure the economic viability of the United States domestic industrial base, including research and development in critical technologies (including critical components for 5G equipment) and workforce development in 5th and future generation wireless communications systems and infrastructure.

Many of the activities outlined in the National Strategy to Secure 5G, and in this implementation plan, will help to directly and indirectly ensure the viability of the United States industrial base, much of which has been acquired by foreign corporations as a result of industry consolidation, or has been significantly off-shored, as is the case with advanced microelectronics. In particular, Activity 1.1 of this

implementation plan provides a roadmap to increasing United States technological competitiveness in telecommunications. Similarly, Activity 4.6 describes how the United States Government will work with the private sector, academia, and international government partners to adopt policies, standards, guidelines, and procurement strategies that reinforce 5G vendor diversity to foster market competition.

Lead Entity: EOP/NEC

Supporting Entities: OSTP, NSF, DOC, DOJ, FCC, State, USTR, DHS, CISA

Outcome Statement: The United States Government will develop options for incentives and policies to support and bolster the United States industrial base. The United States Government will promote the viability of the United States domestic industrial base through frequent engagement with the private sector and evaluation of commercial, security, and technological developments in 5G networks

Activity 3.3: Address the risk of 'High-Risk' vendors in United States 5G infrastructure (forward looking).

This activity outlines how the United States Government will address the risk of high-risk vendors in the United States. This activity includes, but is not limited to, leveraging mechanisms such as the Implementation of E.O. 13873, on "Securing the Information and Communications Technology and Services Supply Chain." The implementation of this E.O. is designed to complement activities by the Committee on Foreign Investment in the United States (CFIUS), the Federal Acquisition Security Council (FASC), and Team Telecom reviews of Federal Communication Commission licenses involving foreign ownership. The United States Government will leverage these and additional activities to address the risk of high-risk vendors in the 5G infrastructure.

Lead Entity: CISA

Supporting Entities: DHS, ODNI, DOJ, FCC, State, ODNI-directed IC agencies

Outcome Statement: Networks in the United States will be built by trusted vendors and with trusted equipment and technologies. Trusted vendors will be economically viable and contribute to the development of a robust and secure 5G ecosystem. The United States Government will facilitate increasing the number of trusted vendors in the 5G marketplace and address risks posed by limited or unfair competition.

Activity 3.4: Private sector engagement on 5G security.

This activity outlines 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.

Lead Entity: DOC

Supporting Entities: DHS, CISA, FCC, Sector Specific Agencies (SSAs), Relevant IC entities including FBI and NSA.

Outcome Statement: Critical infrastructure stakeholders gain an understanding of the risks associated with 5G technology and make informed, risk-based strategic security decisions. Similarly, United States Government gains an understanding of efforts the private sector may face in addressing or mitigating these risks.

Activity 3.5: Establish acquisition processes to facilitate 5G infrastructure for classified information requirements.

This activity is intended to identify key actions necessary to provide classified 5G infrastructures that leverage, to the maximum extent practicable, unclassified 5G infrastructures that support United States national security interest.

Lead Entity: GSA

Supporting Entity: DOD, other appropriate United States Government Agencies

Outcome Statement: Best In Class (BIC) acquisition vehicles(s) to support infrastructure for classified information handling that leverages secure 5G infrastructure. United States Government agencies will identify their standards, security controls, and other requirements to provide a secure infrastructure for classified networks. This effort is intended to reduce cost and eliminate acquisition redundancies.

Line of Effort Four: Promote Responsible Global Development and Deployment of 5G

The United States will work with international partners to lead the responsible international development and deployment of 5G technology and will work to promote the availability of secure and reliable equipment and services in the market.

Activity 4.1: Diplomatic engagement plan for risk mitigation, standards, and security principles.

This activity outlines an approach for diplomatic engagement with mutual defense treaty allies, strategic partners, and other countries to share security risk information and findings pertaining to 5th and future generations wireless communications systems and infrastructure equipment and cooperation on mitigating those risks. This activity seeks to promote interoperability, competitiveness, openness, and secure platforms.

The United States employs a multi-pronged effort to promote responsible global development and deployment of secure 5G networks. The primary component of this campaign involves sharing information and assessments of the risks, vulnerabilities, and threats associated with 5G networks and untrusted vendors that are subject to influence or control by a third government without democratic or independent judicial checks and balances. The campaign also includes highlighting complicity in human rights abuses, intellectual property theft, and sanctions violations activities by untrusted vendors, such as Huawei and ZTE, to underscore why these firms cannot be trusted and should be prohibited from critical 5G networks.

The United States Government employs a layered advocacy campaign that includes bilateral outreach to allies and partners, multilateral coordination through existing organizations and new initiatives (e.g., the Prague 5G Security Conference), and broader communications and outreach efforts to businesses and the public. The goal of this diplomatic engagement is to convince allies and partners to adopt and implement 5G security measures that effectively prohibit the use of untrusted vendors in all parts of 5G networks, while improving network security, openness, interoperability, performance, and global connectivity. A detailed Diplomatic Engagement Plan is included in Annex B. Activities that fall under this plan include:

1. Raise awareness among allies and partners on security risks
2. Encourage allies and partners to take concrete actions to protect their 5G networks
3. Encourage use of trusted 5G vendors
4. Partner with like-minded countries
5. Public diplomacy
6. Promote the Prague Proposals
7. Multilateral engagement
8. Encourage allies and international partners to implement the Department of State 5G Clean Path initiative

Lead Entity: State

Supporting Entities: DOD, DOC (NIST, NTIA, ITA), DHS, CISA, USTR, FCC, USAID, and FBI

Outcome Statement: Adoption of secure, trusted 5G networks globally that are free of untrusted vendors in all parts of the network; and the promotion of global 5G vendor diversity for a robust, secure 5G ecosystem.

Activity 4.2: Provide Technical Assistance to International Partners.

This activity outlines an approach to provide technical assistance and financing support to eligible private sector companies, mutual defense treaty allies, and strategic partners of the United States, and other countries, when in the security and strategic interests of the United States, to maximize the security of 5th and future generations wireless communications systems and infrastructure inside their countries. In addition, this activity addresses the need to provide competitive deal financing for trusted vendors through EXIM and DFC to level the playing field against the substantial state subsidies and financing that some untrusted vendors receive. The goal of this activity is to provide a comprehensive set of financing support, technical assistance, and expertise that empowers countries to implement 5G security measures and procure equipment from trusted vendors.

Key areas of focus include leveraging the Digital Connectivity and Cybersecurity Partnership (DCCP) for whole of government technical assistance and programming, providing competitive deal financing, and coordinating advocacy for trusted vendors. A detailed plan is provided in The Technical Assistance Plan for International Partners (Annex C).

Lead Entity: State

Supporting Entities: DFC, DOC, DOD, DOJ, DHS, CISA, EXIM, FBI, FCC, USAID, USTR, and USTDA

Outcome Statement: Partner countries and eligible private sector companies invest in and deploy secure and trusted 5G ecosystems facilitated, as appropriate, with United States Government support, assistance, and expertise, enabling countries to develop their telecommunications infrastructure with secure, and trusted 5G and next generation networks that are free of untrusted vendors and that increase global connectivity.

Legislative Action Required: Consider appropriating adequate funding for a 5G security fund to enable the Secretary of State, EXIM, and DFC to work with eligible private sector companies and like-minded countries to assist allies and partners in adopting trusted and secure telecommunications equipment and offsetting the costs of procuring equipment from trusted vendors.

Activity 4.3: Mitigating the security risk from untrusted equipment in international partners' systems.

This activity addresses options for identifying and helping to mitigate the security risks of 5th and future generations wireless communications systems and infrastructure that have security flaws or vulnerabilities, or are utilizing equipment sourced from countries of concern, and that have already been put in place within the systems and infrastructure of mutual defense treaty allies, strategic partners, and other countries, when in the security interests of the United States.

Lead Entity: State

Supporting Entities: DOC, DOD, FCC, DHS, CISA, DOJ, NSA, and ODNI

Outcome Statement: Countries and mobile network operators fully recognize the risks of using untrusted vendors in any part of a 5G or next generation network and take appropriate actions to address

the risks, including actions to remove and replace ICTS so as to reduce or eradicate equipment supplied by untrusted entities from 5G network infrastructure.

Activity 4.4: Promote United States leadership in international standards development for 5G, including through private sector and international engagement.
This activity outlines how the United States Government will work to preserve and enhance United States leadership on 5G in relevant organizations that set standards. This activity will be conducted in concert with the private sector, including but not limited to commercial, academic, and like-minded international partners. This will include efforts such as expanding Federal departments and agencies coordination and participation in standards-setting organizations. The United States will emphasize the need for open and transparent processes to develop timely, technically robust, and appropriate standards.

Annex D provides a detailed plan for engagement with private sector communications infrastructure, systems equipment developers, and academia to encourage the maximum participation possible by the private sector on standards setting bodies related to such systems and infrastructure equipment standards by public and private sector entities from the United States.

Specific efforts in this plan include:

1. Identify key United States Government standards engagements
2. Identify and articulate Federal Government 5G standardization priorities
3. Strengthen United States Government capacity for standards engagement
4. Prioritize and help strengthen United States Government engagement, coordination, and information exchange
5. Strengthen coordination with the United States private sector
6. Strengthen diplomatic engagement on standards and international coordination
7. Develop options to encourage participation in standards setting bodies by reducing barriers to private sector participation in standards development activities

Lead Entity: DOC/NIST

Supporting Entities: DOC (NTIA, ITA), State, DOD, DOJ, DOT, DHS, CISA, FCC, USTR, FBI, and NSA

Outcome Statement: United States and international partners will effectively influence international standards through expanded and increased participation in private and international 5G engagements.

Activity 4.5: Joint testing environments with international partners.

This activity outlines efforts 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. The United States Government will engage with international allies and partners to shape the outcomes of 5G and beyond systems and services. Federal agencies will work closely with State to utilize multilateral and bilateral dialogues to collaborate with international partners, identify 5G and beyond security vulnerabilities, develop shared testing capabilities, demonstrate secure 5G and beyond technologies, and share relevant threat intelligence with appropriate entities. Additional complementary actions are described in Activity 4.6.

Lead Entity**:** OSTP

Supporting Entities: State, DOD, NSF, DOE, DOT, USDA, DOC, NIST, NTIA, DHS, and FCC

Outcome Statement: The United States Government in collaboration with international partners, will establish programs that address 5G security and vulnerability challenges associated with 5G components. The United States Government will collaborate with international partners to jointly test and demonstrate 5G and beyond technologies, concepts, and applications of interest for the government (including defense), academia, and commercial sectors. This includes partnering with like-minded countries to share expertise in creating effective testing and measurement environments, aligning 5G and beyond R&D agendas, updating and expanding testing facilities and methodologies to accommodate internationally based programs, and conducting R&D activities in the United States that are coordinated with foreign partners to accelerate deployment of 5G applications and use-cases.

Activity 4.6: Policies and strategies for global market competitiveness and diversity of secure 5G infrastructure.

This activity outlines how the United States Government will work with the private sector, academia, and international government partners to adopt policies, standards, guidelines, and procurement strategies that reinforce 5G vendor diversity to foster market competition. The United States Government will join private sector and international partners in designing market-based incentives, accountability mechanisms, and evaluation schemas to assess diversity, component transparency, fair financing, and competition across the 5G technology landscape as a means to better secure the global network.

The United States Department of Commerce will work with the United States Government departments and agencies to develop and deploy an array of programs and tools to promote United States technology solutions in the global market, work to remove and reduce trade and regulatory policies that harm United States companies' international competitiveness, provide support for trusted vendors, and advocate for policies and regulations that promote open, competitive markets for United States technology companies. The strategic framework for this activity is outlined in Annex E. Key objectives of the strategic framework include:

1. Enhance organization capacity and resources to accomplish strategic objectives.
2. Increase and diversify the participation of United States companies in the global communications infrastructure market.
3. Collaborate with partner countries to support trusted vendors in the global communications infrastructure.
4. Collaborate with like-minded countries on policy options to advance the development and deployment of open interfaced, standards-based, and interoperable 5G networks as a means to create innovation, spur competition, and expand the 5G supply chain.
5. Expand and bolster government and industry engagement with international partners on policy and the regulatory environment for enabling the 5G technology ecosystem.
6. Enhance and expand bilateral and multilateral assistance programs with international partners specific to promoting the deployment of digital innovations for communications infrastructure.
7. Development of metrics to track the progress and accomplishment of strategic framework objectives.

Lead Entity: DOC/ITA & NTIA

Supporting Entities: State, DHS, CISA, FCC, DOJ, NSF, DOD, DOC/USPTO, GSA, and others

Outcome Statement: The United States Government fosters a competitive global ecosystem for trusted 5G vendors. The United States Government promotes vendor diversity and collaboration on 5G innovation with international partners. Employ a strategic framework to increase and diversify the participation of United States companies competing in international 5G technology markets, provide support to other trusted vendors, and expand policy engagement with international partners to establish open, competitive markets for United States technology companies in international markets.

ANNEX A

A Plan for Research, Development, and Testing to Reach and Maintain United States Leadership in Secure 5G and Beyond (Activity 1.1)

Lead Entity: OSTP

Supporting Entities: DARPA, DHS, CISA, DOD, DOE, DOL, DOT, State, ED, FBI, FCC, FDA, FMG, NIST, NSA, NSF, NTIA, and ODNI.

This research plan provides focus for the Federal and national research efforts to advance and sustain United States leadership in 5G and beyond technologies and to secure the national 5G and beyond infrastructure. The principal risks and challenges to United States competitiveness in securing 5G and beyond include: (1) supply chain vulnerabilities; (2) closed, proprietary, and heterogeneous technical implementations that limit an understanding of vulnerabilities and create barriers to innovation; (3) weaknesses in system architecture and hardware component security; (4) legacy vulnerabilities; and, (5) a limited domestic supplier and manufacturing base. While current approaches to securing critical systems have focused on being reactive, the R&D actions described here seek to institutionalize a proactive, principled, design-centered approach that builds secure 5G and Beyond systems from the ground up and enables the systems to be continually verified and validated. This research plan connects security[3] and resilience, trust, testing and evaluation, standards, education, and IPR as the main aspects of securing 5G and beyond systems.

The United States Government also recognizes that it is essential to build, train, and upskill a workforce to ensure that United States industry, academia, and government have access to the knowledge and skills needed to lead in secure 5G and beyond foundational R&D, compete in the 5G and beyond marketplace, and to prevent national security risks. A trained workforce requires partnerships with United States academia and industry to: ensure appropriate skills training at all stages; develop curricula based on research and real-world challenges; incorporate state-of-the-art software engineering methods; devise, coordinate, and implement training and technology transfer activities; combine technology, business, and policy aspects of security; and cultivate the critical thinking and analytical skills needed to ensure the security of 5G and beyond systems. All activities proposed in this plan are expected to play a role in fostering the development of educational and instructional materials; supporting fellowships, research experiences, and traineeship opportunities; strengthening existing public and private educational and upskilling programs; encouraging the study of STEM fields; and to align with Federal strategies and efforts (e.g., STEM Education[4] and cybersecurity workforce[5]) that contribute to advancing secure 5G and beyond technologies.

---

[3] NSTC. December 2019. *Federal Cybersecurity Research and Development Strategic Plan*, https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf

[4] OSTP. October 2019. *Progress Report on the Federal Implementation of the STEM Education Strategic Plan*, https://www.whitehouse.gov/wp-content/uploads/2019/10/Progress-Report-on-the-Federal-Implementation-of-the-STEM-Education-Strategic-Plan.pdf

[5] White House. May 2019. *E.O. on America's Cybersecurity Workforce*, https://www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/

Plan Details:

1. **Ensure the Security of 5G and Beyond Infrastructure and Services**. To achieve and maintain high security guarantees for 5G and beyond applications and services, including the network edge, a granular 5G and beyond security framework is needed to support the development, verification, validation, deployment, and operation of critical applications and underlying services (referred to in this annex as the "Open Security Framework"). The development of 5G and beyond technologies within this security framework should be underpinned by a domestic innovation and manufacturing base and could be supported by the envisioned new Manufacturing USA Institute for Secure 5G and Beyond Development. To enable security of 5G and beyond infrastructure, services, and applications, the United States Government can facilitate the development of:

    a. An Open Security Framework that: enables continuous validation of 5G and beyond deployments that use commercial technologies across a variety of missions; scales with the number of users/devices; and supports dynamic adaptation to changes across cybersecurity, critical infrastructure, automation, and human interaction with 5G and beyond systems.

    b. A United States-based nexus for nurturing technological innovation and expanding the domestic supplier base for technologies and services conforming to the Open Security Framework. Using a large-scale industry-academia partnership model through a new Manufacturing USA Institute for Secure 5G and Beyond Development to share costs would reduce market and investment risks, provide a locus for R&D and its supporting elements, and foster a domestic capability for secure 5G and beyond systems.

    c. Specific use cases for deployment of 5G and beyond systems in critical domains. Partnerships of mission-specific agencies and industry would emphasize security, safety, privacy, and resilience.

    d. Advanced techniques such as secure virtualization and zero-trust methods to address the security of 5G and beyond systems and the security in micro-services for embedded and highly secure system components.

    e. Technologies to enable secure and dynamic provisioning and management of heterogeneous, software-defined, and virtual hardware and network resources across multiple physical infrastructure components controlled by a variety of service providers. These technologies would also address applications that may have legacy, proprietary, and embedded mission specific aspects.

    f. Adequate evaluation methods for 5G and beyond system integration in mission critical applications that are necessary in the development and regulatory evaluation of critical devices (e.g., medical or cooperative automated transportation safety devices).

    g. Advanced physical layer models, techniques, and designs for: (1) high-quality measurement technologies (up to terahertz frequencies), including RF signals, propagation, test methods, modeling platforms, reference implementations, and training datasets, to support the development, evaluation, standardization, and testing of end-to-end real-time applications; (2) integrated validation and verification frameworks for propagation and channel models, protocols, hardware, and software as part of the design and development process; and (3) security of

spectrum access, including high-frequency bands (mmWave[6] and terahertz), to mitigate a broad range of physical layer threats, including intentional interference and jamming.[7]

2. Leveraging Public-Private Partnerships. Priority should be given to deepening existing public-private partnerships through United States Government 5G testbeds and field locations that can be made accessible and affordable for use by United States industry and academia. Similar priority should be given to support early-stage R&D through high-end domestic manufacturing capabilities in microelectronics fabrication, packaging, and integration for 5G and beyond systems. Enabling access to a nationwide set of diverse testbeds and manufacturing facilities can allow United States industry, academia, and government to focus resources on technology enhancement, development of solutions, and addressing market needs, and this will reduce the duplicative costs associated with the creation of testbed capabilities by multiple entities. To provide a strong testing foundation, the United States Government can:

a. Leverage a set of accessible and affordable nationwide testbeds (laboratory and field, for software and hardware components, including for test, verification, and experimentation) for United States industry, academia, and government. These would cover 5G and beyond from the physical layer up to and including deployment of novel applications and services, interoperability, and coexistence.

b. Leverage state-of-the-art micro- or nano-electronics fabrication and packaging facilities in the United States that provide affordable access to researchers and engineers from industry, academia, and government labs. These facilities should support research, development, test and evaluation (RDT&E) in fabrication and manufacturing processes that can enable innovations in hardware technologies and use of nontraditional materials specifically for 5G and beyond systems.

c. Enable and coordinate testing and evaluation capacity to prioritize the needs of critical infrastructure and services, such as those for healthcare and medical devices, safety-of-life applications, connected and autonomous vehicles, automated transportation systems, smart cities, electric grids, border security, precision agriculture, and the needs of the United States military.[8]

d. Enable testing and evaluation capabilities that cover multiple dimensions of the 5G and beyond deployment space including variable population densities; terrain types (including test tracks); open source elements; 5G and beyond features (e.g., virtualization of radio access networks and network functions, network slicing, mobile edge computing, massive machine-type communications, ultra-reliable low-latency communications); spectrum (mid-band and mmWave); cybersecurity; large-scale data analytics; and a multitude of cross-industry applications and services.

---

[6] mmWave: millimeter wave bands in the 24 GHz–300 GHz spectrum range

[7] NSTC. May 2019. *Research and Development Priorities for American Leadership in Wireless Communications*, https://www.whitehouse.gov/wp-content/uploads/2019/05/Research-and-Development-Priorities-for-American-Leadership-in-Wireless-Communications-Report-May-2019.pdf, responding to the Presidential Memorandum on *Developing a Sustainable Spectrum Strategy for America's Future*, https://www.govinfo.gov/content/pkg/FR-2018-10-30/pdf/2018-23839.pdf

[8] DOD. May 2020. *Department of Defense (DOD) 5G Strategy*, https://www.cto.mil/wp-content/uploads/2020/05/DOD_5G_Strategy_May_2020.pdf

e. Enable 5G and beyond testing and evaluation capabilities that cover interoperability between Federal and commercial entities (particularly equipment manufacturer and wireless carriers labs); including coexistence, in-band and out-of-band emission susceptibility and effects, and spectrum sharing technologies and systems.

f. Promote resource sharing and access within the Federal 5G and beyond testbeds and with commercial labs to increase utilization and provide multi-domain testing capabilities, and to ensure that all testbeds maximize the leveraging of R&D products and create a common mechanism for information sharing.

g. Coordinate activities of Federal test-beds and testing facilities through a new NITRD sub-working group. The group will be comprised of the respective agencies that oversee Federal 5G and beyond test facilities and act as a platform to share information, coordinate activities, and prioritize activities according to gaps and opportunities within research priorities.

3. Ensure United States Leadership in Secure 5G and Beyond Technologies. To sustain United States technology leadership and readiness for new opportunities, basic R&D in 5G and beyond technologies is critical, as well as in the related hardware and software ecosystems and security. 5G and beyond enables increased wireless connectivity, performance, and reliability of industrial and mobile edge systems. Future-generation communications systems and networks will continue the trend of performance increases with higher capacities, increased device densities, reduced latencies, and lower energy consumption. To spur continued innovation, foundational research should prioritize novel approaches for security, privacy, resilience, and secure-by-design methods. Advancing 5G and beyond technologies will also require increased collaboration with trusted international partners, industry, and academia. To support rapid development of 5G and beyond technologies and their associated hardware and software ecosystems, the United States Government can:

a. Consider investing in new Secure NextG Research Centers that can engage and coordinate multi-domain experts in microelectronics, communication networks, wireless systems, signal-processing, software engineering, formal methods, AI, device identity management, radio frequency (RF) fingerprinting, trustworthy hardware design, and cybersecurity directly aligned with 5G and beyond systems and for the specific purpose of building integrated secure-by-design 5G and beyond systems with provable end-to-end security guarantees. The Centers' expertise should target different 5G and beyond verticals and use cases. Research priorities for such Centers could be modeled after the Computing Community Consortium's research roadmap for 5G security and privacy.[9]

b. Prioritize foundational research activities to develop principled security-by-design approaches that can facilitate and enhance end-to-end security. These approaches will be based on formal methods (including logic reasoning, specification, design, program analysis, verification, synthesis, and programming language-based approaches) to provide security and privacy guarantees for both software and hardware systems.

[9] Computing Community Consortium. March 2020. *5G Security and Privacy – A Research Roadmap*, https://cra.org/ccc/wp-content/uploads/sites/2/2020/03/5G-Security-and-Privacy-A-Research-Roadmap.pdf

c. Support the development, evaluation, standardization, and testing of end-to-end high-speed, low-latency, communications use cases with strong security and privacy requirements, including mobile-edge computing, autonomous-device operations, and heterogeneous device-to-device communications.

d. Develop techniques for a secure software ecosystem. This can include: (1) designing safe and secure programming languages, toolchains for software security, formal methods to verify system design, deployment, or operations; (2) developing new technologies that enable faster, more affordable development and evolution of low-defect software, with the focus on enabling software evolution throughout development and operation in response to changing markets and technologies; (3) advancing R&D in network-aware and energy-aware programming environments to support high levels of device heterogeneity, programmability, and security; and (4) developing tools for plagiarism detection and code obfuscation. Secure and robust software development tools can allow low-resourced innovators and startups to choose low-defect components to stay competitive in quickly evolving markets.

e. Develop techniques for analog and digital hardware security, including RF, analog, and mixed-signal techniques, device identity management, component fingerprinting, supply chain verification, and trustworthy hardware design.

f. Develop AI/ML methods to enhance the autonomy, trustworthiness, and cybersecurity defense posture of 5G and beyond systems by using resilient, ethical, explainable, and adversarial AI/ML methods. Invest in R&D for the application of AI/ML in support of autonomous or adaptive communications.[10]

g. Encourage the development of a comprehensive security risk management framework that includes: (1) standardized security and privacy indices and metrics; (2) tools for evaluation of cybersecurity risk; (3) response and forensics tools to mitigate attacks and analyze their origins; and (4) economic models and mechanisms for 5G and beyond security insurance markets including tools for risk ratings.

h. Advance privacy-preserving mechanisms that mitigate leakage of privacy-sensitive information, for example, in the event of network intrusions.

i. Develop quantum communication systems for secure communications on 5G and beyond networks.

j. Participate actively in Open Source communities that enable the 5G and beyond ecosystem. See, for example, the DARPA Open, Programmable, Secure 5G (OPS-5G) Program.[11]

k. Prioritize research to further United States industrial competitiveness, including research done in collaboration with industry to promote the development, deployment, and application of next

---

[10] NSTC. June 2019. *The National Artificial Intelligence Research and Development Strategic Plan: 2019 Update*, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf

[11] https://www.darpa.mil/program/open-programmable-secure-5g

generation communication technologies through the dissemination of measurement technologies, data, calibrations, and standards participation.

l. Protect American innovation by preventing, and combating, and enforcing intellectual property rights theft. Raise awareness of threats, tactics and techniques, and enforcement measures with domestic and international partners to enhance mitigation and efforts to hold malicious actors accountable.

4. Create an Open and Competitive 5G and Beyond Ecosystem. The competitive readiness of the United States industrial enterprise depends on fair market access and reduced barriers to entry. These barriers take the form of high capital costs of developing complex proprietary hardware and software for 5G and beyond systems. It is critical that the United States strengthen the diversity and security of the domestic and allied 5G and beyond supply chain by lowering barriers for entry to startups, small businesses, and other trusted suppliers. This can be achieved by: (1) creating techniques to transition users from legacy, single-vendor systems to modern, multi-vendor, virtualized systems; (2) promoting an open, modular, interoperable, and secure architecture that breaks down dependencies between hardware and software components while maintaining practicality and highest performance; and (3) fostering a strong IPR environment that incentivizes private-sector R&D investment by protecting the R&D results. Collaboration with industry and trusted international partners will also ensure increased interoperability and spur innovation. To enable an open, modular, interoperable, and secure ecosystem, the United States Government can:

a. Utilize zero trust as a defining architectural principle to drive security standards and secure component development of critical 5G and beyond systems.

b. Develop and disseminate measurement and modeling platforms to accelerate the development and deployment of open, integrated, and interoperable functionalities.

c. Prioritize current and future investments in interoperability testing environments (particularly those discussed in actions 2(a)-2(g) of Annex A) for plug-and-play across various 5G and beyond system components and resilience across various cyber-threats.

d. Standardize validation and verification frameworks for protocols, hardware, and software as part of the design and development process. Institutionalize, within standards bodies, the use of formal methods to verify system design, deployment, operation, and compliance specification.

e. Consider investing in open-source software development and open-source solutions for end-to-end network security, along with open reference hardware designs for 5G and beyond systems.

f. Organize and incentivize 5G and beyond innovation efforts across the workforce.

g. Consider establishing a Software Development Center for 5G and Beyond: A Software Development Center for 5G and Beyond would be a new, nationally focused public-private partnership entity that serves as an objective and trustworthy agent to help accelerate the commercialization of new software technologies across the entire networking stack. It would foster an open and competitive integration model for engaging with its stakeholders and leverage the strengths of an open-source software approach, as follows: (1) the Center would work across industry, academia, and government to provide input and connections to software projects, including open-source projects, that address gaps, and develop in coordination with the open-

source communities, best practices for such projects; (2) the Center would work across industry, academia, and government to define challenging problems to build a network of expertise and talent; (3) full-time technical experts and information technology staff working in collaboration with outside experts would support open-source projects and organizations to maintain a wide breadth of expertise. They would manage resources for hosting open-source code and performing continuous integration across multiple types of machines and hardware and develop references, examples, and educational materials; and (4) the Center would execute contracts for different open-source efforts in a consortium (or consortium-like) model via multiple engagement models. Executing Cooperative Research and Development Agreements (CRADAs) with companies would provide a means for funding various efforts.

5. **Standards**. Standards and system architectures are an essential part of the technology lifecycle that support accelerated large-scale, interoperable implementation of R&D results; ensure United States consumers and manufacturers can participate fairly in global markets; transfer technical developments to interoperable products; establish conformance and testing requirements; and identify gaps for future R&D needs. See Annex D for specific actions related to Standards bodies. To accelerate large-scale interoperable implementation of R&D results, the United States Government can:

    a. Provide active, persistent, and coordinated technical participation in essential standards development organizations (SDOs), SDO consortia, voluntary consensus standards organizations, and industry alliances directly related to 5G and beyond core technologies and security, as well as related wireless and non-wireless standards.

    b. Reduce barriers to United States participation in SDOs, SDO consortia, industry alliances, and open source development by working with industry, including small business, and academia to identify and address these barriers (e.g., funding standards participation in grant awards and exploring tax incentives).

    c. Support standards-compliant open reference implementations to advance the iterative standards development process.

    d. Cooperate with countries to promote responsible global technology development of aligned specifications, standards, and compliance testing.

ANNEX B

Plan for Diplomatic Engagement (Activity 4.1)

This Plan outlines activities for diplomatic engagement with mutual defense treaty allies, strategic partners, and other countries to share security risk information and findings pertaining to 5th and future generations wireless communications systems and infrastructure equipment and cooperation on mitigating those risks. This activity includes diplomatic engagement to share information and findings on 5th and future generations wireless communications systems and infrastructure equipment standards to promote maximum interoperability, competitiveness, openness, and secure platforms.

The United States employs a multi-pronged strategy to promote responsible global development and deployment of secure 5G networks. The primary component of this strategy involves sharing information and assessments of the risks, vulnerabilities, and threats associated with 5G networks and untrusted vendors that are subject to influence or control by a government without democratic or independent judicial checks and balances. The United States Government employs a layered advocacy campaign that includes bilateral outreach to allies and partners, multilateral coordination through existing organizations and new initiatives like the Prague 5G Security Conference, and broader communications and outreach efforts to businesses and the public. The goal of this diplomatic engagement is to convince allies and partners to adopt and implement 5G security measures that effectively prohibit the use of untrusted vendors in all parts of 5G networks, while improving network security, openness, interoperability, performance, and global connectivity. Key elements of this plan include:

1. ***Raise Awareness among Allies and Partners on Security Risks***: The Department of State leads department and agency efforts to communicate the range and breadth of risks and threats posed by untrusted vendors that are subject to unchecked control or influence by authoritarian governments, including the People's Republic of China (PRC). This department and agency campaign includes coordinated outreach at senior political levels and robust information sharing between intelligence agencies, ministries of defense, trade and economic ministries, ministries of justice, and ministries of interior. While this is a global campaign, the United States government prioritizes countries for diplomatic engagement based on military alliances, mutual defense treaties, strategic partnerships, market size, economic and trade relationships, and the state of technological development. The United States will also partner with like-minded countries, businesses, and institutions to build global momentum and jointly communicate the risks of untrusted vendor participation in 5G networks.

2. ***Encourage Allies and Partners to Take Concrete Actions to Protect their 5G Networks***: The United States Government shall encourage partners and allies to develop and implement measures that effectively exclude untrusted vendors from all parts of their 5G networks. As such, the United States Government will provide technical assistance, information, expertise, and input to allied and partner governments as they consider, develop, and implement measures to prohibit or restrict the use of untrusted vendors. The Department of State leads the department and agency effort and leverages United States embassies and missions to coordinate communication and assistance with allied, partner, and like-minded governments.

3. ***Encourage use of Trusted 5G Vendors***: In addition to sharing security concerns about untrusted vendors, the United States Government actively encourages countries and mobile network operators to

choose existing trusted vendors, evolve to integrated and open architecture networks, and build interoperability.

4. ***Partner with Like-Minded Countries***: Many United States allies and partners share similar concerns about untrusted 5G vendors and the threats posed by suppliers subject to the control or influence of authoritarian governments. The United States is pursuing public commitments to secure, trusted 5G equipment, architecture, and infrastructure with like-minded governments through memorandums of understanding (MOUs) or joint statements. These MOUs and joint statements form a basis for further cooperation on 5G security between the United States and these governments, including outreach and advocacy to other countries. These efforts help build momentum and demonstrate global consensus on the importance of 5G security.

5. ***Public Diplomacy***: In addition to government-to-government engagement, the 5G security campaign includes public outreach to influence the private sector, academia, and the public. This outreach seeks to increase public understanding of the security risks associated with untrusted vendors and to pressure governments and businesses to protect their security and privacy online. Public diplomacy and public affairs were key components of the successful efforts in late 2019 to encourage the European Union to release a strong 5G Security Toolbox, which provided a list of recommended measures nations should adopt to protect their 5G networks and address the risks posed by untrusted, high-risk vendors. The EU and its member states will continue to be a priority for the United States 5G campaign. Public diplomacy includes speaker exchanges, International Visitor Leadership Programs, embassy hosted events, and other similar programs.

6. ***Promote the Prague Proposals***: In May 2019, the Czech Republic hosted representatives from nearly 40 countries for the international Prague 5G Security Conference. The conference was organized around four pillars: i) policy; ii) technology; iii) economy; and iv) security, privacy, and resilience. At the conclusion of the conference, the "Prague Proposals" were released and endorsed by the United States. These proposals provide a guide for how countries should build secure and resilient 5G networks based on free and fair competition, transparency, and the rule of law. The United States Government continues to encourage allies and partners to endorse the Prague Proposals and to use them as a guide for telecommunications regulation. These proposals are also enshrined in bilateral MOUs and joint declarations on 5G security between the United States and like-minded countries. Furthermore, the United States will participate in future Prague 5G Security Conferences.

7. ***Multilateral Engagement***: In addition to bilateral engagements, the United States engages in multilateral fora to promote secure, trusted, open, integrated, and interoperable 5G networks globally. The United States will continue to raise security concerns in the North Atlantic Treaty Organization (NATO) and seek to harmonize security policies across NATO Allies to ensure they collectively and individually prohibit the use of untrusted vendors. In addition to NATO, the United States Government will also work through organizations like the Organization for Economic Co-operation and Development, (OECD), the Asia-Pacific Economic Cooperation (APEC), Association of South East Asian Nations (ASEAN), and other organizations to build consensus for principles of trust, security, openness, integration, interoperability, transparency, and resilience in 5G and other next generation networks.

8. ***Encourage Allies and Partners to Require a "5G Clean Path" for Overseas Facilities***: On April 29, 2020, Secretary of State Michael Pompeo introduced the 5G Clean Path initiative to protect the data and networks of United States diplomatic facilities at home and abroad. The 5G Clean Path envisions an

end-to-end communication path that does not use any transmission, control, computing, or storage equipment from an untrusted vendor. The United States Government will require a 5G Clean Path for diplomatic and potentially other government facilities domestically and abroad. In addition, the United States Government will urge other countries and private businesses in critical sectors to require a 5G Clean Path for their own communications to ensure security and confidentiality and to prevent the theft of intellectual property. The goal of the 5G Clean Path initiative is to demonstrate the demand for secure, trusted telecommunications networks and to create a business imperative for mobile network operators to build networks using only trusted vendors.

Lead Entity: Department of State

Supporting Entities: DHS, CISA, DOC, DOD, FCC, FBI, ODNI, USTR, and USAID

ANNEX C

Plan for Technical Assistance for International Partners

(Activity 4.2)

This plan outlines a framework and architecture for providing technical assistance to international partners. This plan is led by the Department of State in coordination with USAID, the United States Export-Import Bank (EXIM), the United States International Development Finance Corporation (DFC), the United States Trade and Development Agency (USTDA), and the Department of Commerce, and focuses on two main activities:

1. The Digital Connectivity and Cybersecurity Partnership, and
2. Competitive Financing for Trusted Vendors.

***The Digital Connectivity and Cybersecurity Partnership*.** In December 2017, NSC Principals endorsed a Roadmap drafted by the Department of State and USAID to counter the influence of the PRC and other authoritarian powers in the areas of internet governance, Information and Communications Technology (ICT) infrastructure development, and cybersecurity. To support the Roadmap, State and USAID developed the Digital Connectivity and Cybersecurity Partnership (DCCP), which was formally launched and funded by Secretary Pompeo in 2018. The DCCP is a global, multi-year, whole-of-government effort coordinated by State to promote access to an open, integrated, interoperable, reliable and secure internet, including 5G and other emerging digital technologies. DCCP is the umbrella initiative under which a majority of programming on 5G is funded and coordinated. The Department of State is launching a number of programs under the DCCP using FY 2019 funding to support the 5G campaign.

Department of State programming, through contracts and department and agency agreements, will provide legal and regulatory advisory services to assist countries in developing and implementing laws, regulations, and other measures on 5G security. State will also support capacity building trainings and workshops for developing-country government officials on 5G security with participation from experts from the private sector, like-minded foreign governments, academia, and the United States Government. This assistance will be provided on a bilateral, regional, and multilateral basis. State and departments and agencies will continue to identify programmatic opportunities to support the 5G campaign under DCCP.

United States Agency for International Development (USAID) programming will promote open, interoperable, reliable, and secure communications networks and build cybersecurity capacity in USAID recipient countries. Pursuant to its Digital Strategy, USAID will use its unique relationships with host country governments - relationships that extend beyond ICT ministries to include health, education, and economic policymakers - civil society, and the private sector to advance trusted telecommunications networks. Specifically, USAID will (1) develop strategies to help countries adopt ICT and digital economy policies that advance an open, interoperable, reliable and secure cyberspace; (2) engage secure network supply alternatives using private sector investment and innovation models; and (3) work with implementing partners to ensure safe access to technologies and the Internet.

***Competitive Financing for Trusted Vendors*.** Information and Communications Technology and Services (ICTS) network deployments are capital intensive. Untrusted vendors, including Huawei and ZTE, benefit from government financing for deployments in China (e.g., R&D and capital equipment acquisition) and for working capital needs. This domestic financial support, combined with preferential access to the Chinese market enables these vendors to offer lower cost financing terms and, in some cases, below-market export credit subsidies to foreign mobile operators to purchase their equipment. The United States Government is working to mobilize the full range of department and agency tools and coordinate with like-minded partners to support foreign mobile network operators in procuring trusted, secure ICTS equipment.

United States Export-Import Bank (EXIM) will support United States exports of 5G technologies by providing (1) loan guarantees, (2) trade credit insurance, (3) working capital guarantees, and (4) direct loans. EXIM can work in a wide range of markets, offering support for public and private sector borrowers to procure trusted 5G equipment and services with United States content. EXIM will maintain a series of co-financing structures with partner export credit agencies from like-minded countries such as Korea, Japan, Finland, and Sweden to support 5G procurement from United States vendors and trusted vendors from other countries. Where feasible, EXIM will collaborate with export credit agencies from partner countries to offer streamlined joint financing for projects that include content from both countries. EXIM has joint finance agreements with sixteen export credit agencies and does not require a standing agreement to co-finance deals with other export credit agencies.

EXIM will support viable deals that comply with OECD guidelines. When there is evidence of a competing offer with State-backed financing terms that are more generous than those allowed under OECD export credit rules, EXIM would consider, under the auspices of its new Congressionally mandated Program on China and Transformational Exports (the Program), matching a Chinese competitor's financial terms to help level the playing field for United States exports. Under the Program, EXIM will support United States innovation, employment, and leadership in next generation wireless communications equipment and services.

The United States International Development Finance Corporation (DFC) will continue to partner with United States and foreign private sectors to provide financing solutions to private companies in countries seeking to build out 5G networks. Information and communications technology is a priority sector for DFC. DFC financing solutions can help secure market entry and presence for trusted vendors and promote an open and secure global communications network, including by investing in the rollout of new architectures such as virtualized networks. DFC's products include (1) equity financing (directly or through targeted investment funds) for developmentally and strategically significant companies and projects; (2) debt financing through direct loans and guaranties (with specific programs targeting small and medium business); (3) political risk insurance to protect investments against losses due to currency inconvertibility, governmental interference, and political violence; and (4) technical assistance to accelerate project identification and preparation to attract and support private investment. USAID will continue to collaborate with the DFC's Mission Transaction Unit to support secure network connectivity investments and private sector partnership opportunities in countries where USAID has a development presence.

The United States Trade and Development Agency (USTDA) will deploy technical advisory services to evaluate and develop recommendations for project preparation related to enabling,

developing, deploying, or upgrading secure and sustainable next generation, including 5G, networks. For international infrastructure project preparation, USTDA: (1) performs feasibility studies; (2) provides technical assistance and comprehensive analyses of technology options and requirements; and (3) supports pilot projects that test commercially viable United States technology.

In addition to project preparation, USTDA will continue to employ a range of tools to support the 5G security campaign, such as: training grants, reverse trade missions, and technical workshops and conferences to connect United States companies to next generation network projects and export opportunities in low to middle income countries. For international infrastructure tenders, under limited circumstances, USTDA can provide support to United States firms competing for a tender via a "training grant" if it is found that United States firm(s) face an uneven playing field and competitive disadvantage due to non-United States competitors offering incentives to the project sponsor (beyond the tender requirements) made possible by governmental support. Through reverse trade missions, USTDA brings foreign project sponsors to the United States to observe the design, manufacture and operation of United States products and services that support their infrastructure goals. USTDA's sector and region-specific technical workshops and conferences connect United States firms with foreign buyers, highlight upcoming overseas infrastructure projects, and showcase United States goods and services.

The Department of Commerce (Commerce) will continue to promote and strengthen the competitiveness of United States technology companies in the global 5G market. Commerce will use various programs and tools as specified in the strategy framework for Activity 4.6 and Annex E to promote United States technology solutions in foreign markets, work to remove and reduce trade and regulatory policies that harm United States companies' international competitiveness, and encourage industry-driven, market-based standards that are the foundation of United States technology leadership. Commerce will continue to advocate for regulatory regimes concerning intellectual property protection, conformity assessment, privacy rules, and other policies that promote favorable commercial environments for United States companies to expand business opportunities and increase the prevalence of United States-sourced technology in global communications networks. Commerce's Commercial Law Development Program (CLDP), with funding and guidance from State, will create a reference guide of successful actions taken by countries around the world to secure their 5G networks and engage with ally and partner countries on a bilateral and regional basis.

ANNEX D

Plan to Promote United States Leadership in International Standards Development for 5G and Beyond (Activity 4.4)

This plan intends to stimulate United States Government and private sector leadership in international standardization for 5G and beyond communication technologies to ensure that the resulting standards are state-of-art, fit-for-purpose and are developed in open, transparent, consensus-based processes that are not subject to malign influence by state-actors or their proxies. Specific efforts in this plan include:

1. Identify key United States Government standards engagements
2. Identify and articulate Federal Government 5G standardization priorities
3. Strengthen United States Government capacity for standards engagement
4. Prioritize and strengthen United States Government engagement, coordination and information exchange
5. Strengthen coordination with the United States private sector
6. Strengthen diplomatic engagement on standards and international coordination
7. Develop options to encourage participation in standards setting bodies by reducing barriers to private sector participation in standards development activities.

1. Identify key United States Government standards engagements

There are a number of international standards organizations, such as 3GPP and multilateral organizations, such as the ITU, that develop 5G and related standards. These organizations and the working groups within which the deliberations take place operate differently. NIST will lead a department and agency effort to gather data and analyze important metrics within these bodies and working groups. This data will be collected and analyzed to help identify standardization activities where greater or more effective United States engagement is necessary. This initial step will also involve recommending methodologies for ongoing monitoring and data collection to help the United States identify any emerging risks around participation trends and allow for a proactive response.

Lead Entity: Department of Commerce - NIST

Supporting Entities: DOC/NTIA, DOC/ITA, State, DHS, CISA, USTR, FCC, DOT, DOD, and NSA

Outcome Statement: Enhanced United States Government understanding of ongoing standards policy development opportunities for United States Government and stakeholder contributions. Participants and standards development organizations follow the principles of consensus, openness, due process, transparency and stakeholder balance. Standards development organizations are not effected by attempted foreign governmental takeover or undue influence counter to the open principles stated above.

2. Identify and articulate Federal government 5G standardization priorities

To ensure 5G standards meet the United States Government's interests for secure 5G deployment, the United States Government needs to identify its standards' needs. United States Government's interests in 5G-related technologies and associated applications will vary widely depending on Federal agencies' missions. Such identification and prioritization will also enable United States Government to refine plans for United States Government staffing and engagement in important standardization activities and

to allow for more targeted coordination across Federal agencies. This activity also will allow United States Government to better convey its priorities to its private sector partners so United States Government and the United States private sector can more effectively collaborate in standards development activities.

Lead Entity: DOC/NIST

Supporting Entities: DOC/NTIA, State, DHS, CISA, FCC, NSA, DOT, and USTR

Outcome Statement: Development of a list of priority issues, and organizations/working groups to help guide increased United States Government focus in standards development.

3. Strengthen United States Government capacity for standards engagement

For effective and productive standards engagement, the United States Government needs:

- Staff who are technically proficient in standards development and management support and resources to fully engage in standardization activities.

- In-person participation in standards meetings by technically proficient staff to build working relationships with other standards participants.

- A robust pipeline of ideas and talent to ensure strong United States Government proposals, where appropriate, and support for industry-led engagement on 5G and beyond standardization.

Leveraging existing standards expertise within United States Government, the United States Government shall make available standards training courses for appropriate technical staff who would benefit from training in participating in standards development activities. This training should touch on factors that directly contribute to effective participation and engagement in standardization. The United States Government will conduct standards briefings for agency senior executives who have decision-making authority relating to standards engagement and resourcing such engagement. Agency senior executives shall seek to support staff participation as well as recognize and reward leadership and initiative by federal staff who contribute to the achievement of standards related objectives. Federal agencies will undertake efforts within their agencies to identify work streams either underway or planned that could result in proposals for new standards development activities in priority areas to further help identify and plan for future staffing needs and training requirements.

Lead Entity: DOC/NIST

Supporting Entities: DOC (NTIA, ITA) State, DHS, CISA, DOD, NSA, USTR, OPM, DOT, and FCC

Outcome Statement: The United States Government is adequately and appropriately represented at priority standards bodies.

4. Prioritize and strengthen United States Government engagement, coordination, and information exchange (ongoing)

The broad expertise of United States Government agencies can make the United States Government a very potent participant in standards development. However, the effectiveness of United States

Government engagement depends on how well agencies are coordinated and sharing information. Strengthened and more targeted coordination helps ensure that United States Government has adequate representation in priority activities, and that Federal agency representatives are working towards shared goals, and not inadvertently weakening United States Government positions. The United States Government will further strengthen department and agency coordination mechanisms, including leveraging the department and agency 5G policy process and its sub-groups, specifically the Standards sub-PCC, and will also look to leverage other department and agency mechanisms such as the Interagency Committee on Standards Policy (ICSP), the Trade Policy Staff Committee, etc. This effort also will include strengthening existing standards body-specific coordination and information exchange mechanisms, such as those relating to United States Government participation in 3GPP, IETF, IEEE, and ITU-T. These efforts will engage staff from State and DOC at United States missions in key countries and markets to ensure the United States Government standards body engagement is well informed by developments in these markets and that these foreign service officers can amplify messaging about United States Government's standards approaches, as appropriate, and priorities to governments and private-sector stakeholders in these markets.

Lead Entity: DOC/NIST

Supporting Entities: DOC (NTIA, ITA), State, DHS, CISA, NSA, USTR, DOD, DOT, and FCC

Outcome Statement: The United States achieves improved effectiveness in stewardship of the development of standards to be open and fair and thus favorable to United States national interests.

5. Strengthen coordination with the United States private sector (ongoing)

The private sector is what drives the historic United States leadership in standards development. Therefore, United States Government coordination with the private sector is imperative to ensure United States leadership in 5G and beyond standardization. To ensure such coordination, United States Government shall improve its ongoing regular information exchanges with the private sector by identifying key coalitions or partnership opportunities, articulating United States Government standardization priorities and requirements; identifying areas where United States Government can support private sector leadership and engagement in international standardization and vice-versa; actively requesting feedback and input from the private sector; and identifying areas where United States Government interests might be differently aligned from those of the private sector.

Lead Entity: DOC

Supporting Entities: DHS, CISA, USTR, DOD, DOT, and FCC

Outcome Statement: The United States Government will expand and increase participation in private sector and international 5G engagements that focus on international standards developments.

6. Strengthen diplomatic engagement on standards and international coordination

Standards bodies are inherently global not just to ensure they are technically robust, but also to ensure global economies of scale and a globally competitive marketplace. To achieve global acceptance of the resulting standards, successful standards bodies historically promoted openness, balance, due process, appeals process, and consensus. Coordination and information sharing with like-minded partner nations can help to share the burden across geographically and regionally diverse standards bodies. Diplomatic

engagement also can bolster support for international standards development through processes that are transparent, consensus-based, and market driven as opposed to reliance on top-down, government driven approaches or national standards.

The United States Government will create a plan to formalize coordination and information sharing mechanisms, including identifying POCs and standards priorities amongst the Five Eyes nations. This would include consolidating ongoing communication by Five Eyes nations' technical experts who engage in or participate as observers in standards bodies and creating plans to help ensure effective participation for additionally prioritized 5G standards. Information sharing and coordination of standards engagement activities should also include and encourage participation from the private sectors of both the United States and like-minded partners.

United States Government also will develop a diplomatic engagement plan to promote open, transparent and market-driven standardization processes. Such outreach would leverage existing bilateral ICTS or standards related dialogues and build on existing relationships through standards, ICTS development and multilateral fora.

United States Government will also work with Departments of State and Commerce representatives at key Missions to monitor market developments and national or regional standardization strategies and priorities and to identify standard-related POCs and key influencers in key countries to help further strengthen diplomatic engagement and international coordination. Such officers also can amplify messaging about United States Government's standards approaches and priorities to governments and private-sector stakeholders in these markets and gather relevant information in support of this strategy.

Lead Entity: State

Supporting Entities: DOC, DOD, DHS, CISA, FCC, DOT, and USTR

Outcome Statement: Global support for open, transparent, consensus-based and market-driven standards processes. Enhanced information sharing and coordinated participation among likeminded partners regarding 5G standards priorities and activities.

7. Develop options to encourage participation in standards setting bodies by reducing barriers to participation in standards development activities

The United States has been and continues to be a leading contributor to ICTS standards development. United States Government and United States private sector participation in SDOs and has helped ensure that standards are timely, state of the art, fit-for-purpose, technically sound, and that they are developed in organizations and processes that exhibit openness, balance, due process, an appeals process, and consensus. The development and transition to 5G and beyond requires greater participation by

United States Government and United States industry representatives who are technically proficient. In certain standards development organizations and working groups, there has been an increase in participation from other countries seeking to influence international standards development organizations towards standards that do not have technical merit. The United States intends to develop ways to foster increases in United States leadership and facilitate greater participation, representation, and influence by United States stakeholders, as appropriate.

Lead Entity: DOC/NIST

Supporting Entities: DOC (NTIA, ITA), USTR, DOT, and FCC

Outcome Statement: Working with industry and SDOs to identify and reduce barriers to participation leading to greater United States private sector participation and leadership in standards development.

ANNEX E

Strategic Framework for Global Market Competitiveness and Diversity of Secure 5G Infrastructure
(Activity 4.6)

Activities and goals in this framework include:

1. *Enhance Department of Commerce and United States Government organizational capacity and resources to accomplish strategic objectives*: NTIA and ITA will work to continue development of training programs for DOC analysts, trade specialists, commercial officers, and other DOC staff, as well as United States Government department and agency partners as appropriate, to expand organizational knowledge about the market for 5G network technologies, other enabling technologies, and vertical use cases of the 5G ecosystem. New work teams and other organization structures will be established to leverage organization resources, increase market intelligence collection, develop promotion tools and programs, and augment information products and services specific to supporting the competitive position of United States companies in the global communications technology market. This will include dedicated stakeholder engagement to improve messaging and education on 5G issues.

2. *Increase and diversify the participation of United States companies in the global communications infrastructure market*: Programs will be developed and implemented to raise awareness about leading-edge technology solutions available from United States companies and facilitate business development opportunities. Actions and deliverables will include but are not limited to trade missions and reverse trade missions, convening workshops and other forums on emerging technologies for 5G and vertical industry applications and use-cases, promoting foreign direct investment in the United States by trusted companies, advocacy for commercial tenders, and promoting United States company participation in demonstration and test bed trials, and funding R&D activities in the United States that are coordinated with foreign partners to accelerate deployment of 5G applications and use-cases.

3. *Collaborate with International Partner Countries to Support Trusted Vendors in the Global Communications Infrastructure*: Collaborate and build partnerships with and among allied countries and international partners to advocate for the use of technology solutions from trusted vendors in the global communications network. Partnerships and other collaboration may include certain government services and support, where appropriate, including advocacy, export and project financing, and other support activities, prioritizing trusted vendors with substantive United States content or United States presence for R&D and manufacturing.

4. *Collaborate with like-minded countries on policy options to advance the development and deployment of open interface, standards-based, interoperable 5G networks as a means to create innovation, spur competition, and expand the 5G supply chain:* Work with like-minded countries to develop additional 5G alternative suppliers. Collaborate to accelerate the research, development and deployment of open and interoperable solutions in the Radio Access Network (RAN). Coordinate closely through existing mechanisms and appropriate organizations.

5. *Expand and bolster government and industry engagement with international partners on policy and regulatory environment for enabling the 5G technology ecosystem*: Prioritize the removal and reduction of regulations by partners that create barriers to trade and market access issues for United States technology companies. Work with partners, including through the development of information products on 5G policy and regulatory framework, to advance policies that help expand business opportunities for United States technology vendors. Policies such as strong intellectual property protection, best practices on conformity assessment procedures, acceptance of industry-driven standards, risk-based cybersecurity principals, and free flow of cross-border data are some of the key policy enablers.

6. *Enhance and expand bilateral and multilateral assistance programs with like-minded countries and trading partners to promote the deployment of digital innovations for communications infrastructure*: Leverage expertise from across United States Government departments and agencies, academia, United States industry, and knowledge leaders from trusted like-minded partners to develop capacity building, workforce development, and other programs to foster the deployment and commercialization of digital technology innovations for 5G and next-generation networks and services. Develop funding mechanisms to accelerate the replacement of untrusted vendors in partners' telecommunications infrastructure, considering gaps in the existing authorities of the Export-Import Bank and Development Finance Corporation as well as the potential need for a dedicated fund.

7. *Metrics to track the progress and accomplishment of strategic framework objectives include*: completed commercial deals for United States companies, selection of other trusted vendors for technology procurements, trade barriers reduced or removed, relevant bilateral or multilateral engagements, number of trade missions and workshops completed, and level of United States private sector and academic participation in demonstration and test bed trials.

ANNEX F

Summary of Potential Legislative Requirements

Activity 3.2: **Identify incentives and policies to ensure United States industrial base economic viability**

- Develop a plan to increase support for Small Business Innovation Research (SBIR) programs in agencies supporting 5G and next generation network technologies R&D to spur domestic innovation and competition.

Activity 4.2: Provide Technical Assistance to International Partners

- Consider appropriating adequate funding for a 5G security fund to enable the Secretary of State, EXIM, and DFC to work with eligible private sector companies and like-minded countries to assist allies and partners in adopting trusted and secure telecommunications equipment and offsetting the costs of procuring equipment from trusted vendors.

Annex A: A Plan for Research, Development, and Testing to Reach and Maintain United States Leadership in Secure 5G and Beyond (Activity 1.1)

- Assess options for creating a new Manufacturing USA Institute for 5G and Beyond Development to serve as large-scale partnership model among academia and industry to share costs and reduce investment risks. See Annex A, 1(b).

- Conduct measurement science in advanced physical layer models, techniques, and designs. See Annex A, 1(f), 1(g).

- Assess options for expanding access to national testbeds for domestic researchers and companies. See Annex A, 2(a)-2(g).

- Conduct secure wireless technology research. See Annex A, 3(a)-3(k).

- Assess options for new and expanded public private partnerships to speed the development and commercialization of products and technologies across the entire network stack. See Annex A,

Activity 4.4: Develop options to stimulate greater United States private sector engagement in standards

- Develop options, such as grants, tax incentive, or other actions to incentivize increased United States private sector and academia engagement in standards development. See Annex A, 5(b).