

NATIONAL STRATEGY TO SECURE 5G

of the United States of America

MARCH 2020





THE WHITE HOUSE
WASHINGTON, DC

My fellow Americans:

Fifth generation wireless technology, or 5G, will be a primary driver of our Nation's prosperity and security in the 21st century. 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 advancement, however, also ushers new risks and vulnerabilities.

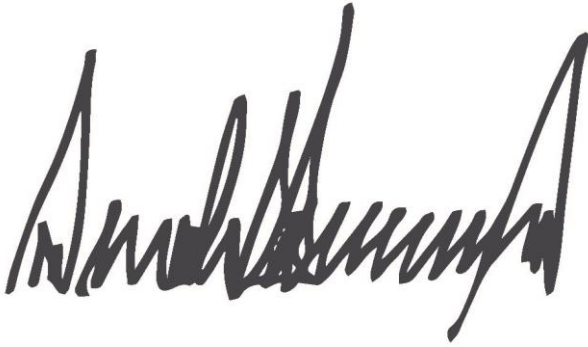
Malicious actors are already seeking to exploit 5G technology. This is a target-rich environment for those with nefarious motives due to the number and types of devices it will connect and the large volume of data that those devices will transmit.

This National Strategy to Secure 5G articulates my vision for America to lead the development, deployment, and management of secure and reliable 5G communications infrastructure worldwide, arm-in-arm with our closest partners and allies, including:

- Facilitating domestic 5G rollout;
- Assessing the risks and identifying core security principles for 5G infrastructure;
- Managing the risks to our economic and national security from the use of 5G infrastructure;
- and
- Promoting responsible global development and deployment of 5G infrastructure.

My Administration is committed to protecting America's national security, promoting our prosperity, and preserving our civil liberties and democratic ideals. Ensuring the security, reliability, and trustworthiness of our 5G infrastructure is essential to these endeavors. This strategy explains how we will do just that.

Sincerely,

A handwritten signature in black ink, appearing to read "Donald Trump". The signature is written in a cursive, stylized font with a large, prominent initial "D".

President Donald J. Trump

The White House

March 2020



Table of Contents

Introduction	1
Line of Effort 1: <i>Facilitate Domestic 5G Rollout</i>	2
Line of Effort 2: <i>Assess Risks to & Identify Core Security Principles of 5G Infrastructure</i>	3
Assess the Risks Posed by Cyber Threats to and Vulnerabilities in 5G Infrastructure	3
Develop Security Principles for 5G Infrastructure in the United States	3
Line of Effort 3: <i>Address Risks to United States Economic and National Security During Development and Deployment of 5G Infrastructure Worldwide</i>	4
Manage the Supply Chain Risks in United States Government Infrastructure, Including 5G	4
Address the Risk of ‘High-Risk’ Vendors in United States 5G Infrastructure	4
Line of Effort 4: <i>Promote Responsible Global Development and Deployment of 5G</i>	6
Develop and Promote Implementation of International 5G Security Principles	6
Promote United States Leadership in International Standards Development and Adoption	6
Incentivize Market Competitiveness and Diversity of Secure 5G Infrastructure Options	6

Introduction

The United States and like-minded countries will lead global development, deployment, and management of secure and reliable fifth-generation (5G) communications infrastructure, which includes hardware, software, and services used to provide 5G. The United States will work with our like-minded partners to establish policies and structures to leap ahead of global industry competitors as 5G standards, 5G technology, and applications that ride on 5G technology evolve.

The United States National Cyber Strategy states that:

The Administration will facilitate the accelerated development and rollout of next-generation telecommunications and information communications infrastructure here in the United States, while using the buying power of the Federal Government to incentivize the move towards more secure supply chains. The United States Government will work with the private sector to facilitate the evolution and security of 5G, examine technological and spectrum-based solutions, and lay the groundwork for innovation beyond next-generation advancements.

This National Strategy to Secure 5G expands on how the United States Government will secure 5G infrastructure domestically and abroad. 5G infrastructure will be an attractive target for criminals and foreign adversaries due to the large volume of data it transmits and processes as well as the support that 5G will provide to critical infrastructure. Criminals and foreign adversaries will seek to steal information transiting the networks for monetary gain and exploit these systems and devices for intelligence collection and surveillance. Adversaries may also disrupt or maliciously modify the public and private services that rely on communications infrastructure. Given these threats, 5G infrastructure must be secure and reliable to maintain information security and address risks to critical infrastructure, public health and safety, and economic and national security.

This National Strategy to Secure 5G will fulfill the goals of the National Cyber Strategy with four lines of effort: (1) facilitating the rollout of 5G domestically; (2) assessing the cybersecurity risks to and identifying core security principles of 5G capabilities and infrastructure; (3) addressing risks to United States economic and national security during development and deployment of 5G infrastructure worldwide; and (4) promoting responsible global development and deployment of secure and reliable 5G infrastructure.

Line of Effort 1:

Facilitate Domestic 5G Rollout

The Administration is facilitating the private sector-led domestic rollout of 5G, primarily coordinated by the National Economic Council. The Federal Communication Commission's (FCC) strategy to Facilitate America's Superiority in 5G Technology (the 5G FAST Plan): (1) makes more spectrum available for commercial use; (2) streamlines government processes for approving 5G infrastructure deployment; and (3) modernizes regulations to promote deployment of 5G backhaul.¹ In addition, the October 25, 2018 Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future directed the Secretary of Commerce to issue a National Spectrum Strategy, which will lay out a long-term plan for spectrum management for 5G and future generations of advanced wireless networks, to include both space and terrestrial systems.

The Administration will also continue to work aggressively with the private sector, as well as like-minded partners and allies to foster and promote the research, development, testing, and evaluation of new technologies and architectures that advance the state-of-the-art technology for 5G and beyond.

¹ <https://www.fcc.gov/5G>

Line of Effort 2:

Assess Risks to & Identify Core Security Principles of 5G Infrastructure

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

Assess the Risks Posed by Cyber Threats to and Vulnerabilities in 5G Infrastructure

The United States Government, in partnership with State, local, and tribal governments as well as private sector partners, will seek to continuously identify and characterize economic, national security, and other risks posed by cyber threats to and vulnerabilities in 5G infrastructure. This effort will include maintaining an understanding of the global 5G market and 5G capabilities and infrastructure, including both space and terrestrial components. This activity will be done with appropriate intergovernmental, interagency, and private-sector engagement.

Develop Security Principles for 5G Infrastructure in the United States

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, and public safety - to United States 5G infrastructure. The principles will be synchronized with other security principles endorsed by the United States Government, such as the “Prague Proposals” from the Prague 5G Security Conference in May 2019.

Line of Effort 3:

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.

Manage the Supply Chain Risks in United States Government Infrastructure, Including 5G

The Federal Acquisition Supply Chain Security Act of 2018 creates a unified, whole-of-government approach to protecting Federal systems from supply chain risks in covered articles, including but not limited to telecommunications equipment and services. Through the Federal Acquisition Security Council created by the Act, the United States Government will identify or develop supply chain risk management standards, guidelines, and practices for executive agencies to use when assessing and mitigating supply chain risks. The Act includes a structure for preventing the use and procurement of sources or covered articles, which may include 5G equipment, in executive agency information systems.

Address the Risk of ‘High-Risk’ Vendors in United States 5G Infrastructure

The United States Government will ensure that 5G and future generations of information and communications technology and services will be deployed in a manner that protects the national security interests of the United States. Executive Order (E.O.) 13873, issued on May 15, 2019, on “Securing the Information and Communications Technology and Services Supply Chain” establishes the authorities to prohibit certain transactions that involve information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary that pose an undue or unacceptable risk to the national security of the United States. The United States Government’s implementation of E.O. 13873 is designed to integrate and synchronize with activities by the Committee on Foreign Investment in the United States, the Federal

Acquisition Security Council, and United States Government reviews of certain Federal Communication Commission licenses involving foreign ownership. The United States Government will leverage these robust activities to address the risk of high-risk vendors in the 5G infrastructure.

Line of Effort 4:

Promote Responsible Global Development and Deployment of 5G

The United States will work with like-minded countries 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.

Develop and Promote Implementation of International 5G Security Principles

The United States Government will participate in the development of international 5G security principles through frameworks, such as the Prague 5G Security Conference. The United States Government will work bilaterally and multilaterally with foreign partners and allies to promote implementation of the 5G security principles within the “Prague Proposals” document that came out of this conference in May 2019.

Promote United States Leadership in International Standards Development and Adoption

The United States Government will work to preserve and enhance United States leadership on 5G in relevant organizations that set standards in concert with the private sector, including but not limited to commercial, academic, and like-minded international partners. This will include efforts such as expanding Federal interagency coordination, participation, and influence in standards-setting organizations. The United States will emphasize the need for open and transparent processes to develop timely, technically robust, and appropriate standards. The United States will promote and support increased participation by the private sector and ensure that such participation is informed by appropriate public-private coordination.

Incentivize Market Competitiveness and Diversity of Secure 5G Infrastructure Options

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-base 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 and protect American values of openness, security, and interoperability.