CISA 5G STRATEGY

Ensuring the Security and Resilience of 5G Infrastructure In Our Nation

2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

CISA 5G STRATEGY

Ensuring the Security and Resilience of 5G Infrastructure In Our Nation

2020

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

> From my perspective, 5G is the single biggest critical infrastructure build that the globe has seen in the last 25 years and, coupled with the growth of cloud computing, automation, and future of artificial intelligence, demands focused attention today to secure tomorrow.

Christopher Krebs
Director, CISA

CISA 5G STRATEGY

CONTENTS

MESSAGE FROM THE DIRECTOR

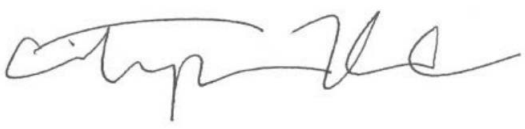
As we look to implement 5G into our nation's networks and critical infrastructure, it is important we work to address potential risks that come with 5G deployment. That is where my agency, the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security (DHS) comes in. CISA leads the national effort to enhance the security, resilience, and reliability of our cyber and physical infrastructure.

As the lead federal civilian agency for cybersecurity, I see our role as being out front as the Nation's risk advisor. And, I use the term "advisor" very deliberately, because it is well known that the private sector owns and operates the majority of critical infrastructure in the United States. Our work with these network defenders takes place on a voluntary basis. Through these partnerships, CISA helps facilitate a collective defense against risks, enabling enhanced capabilities, improved decision making, and increased information sharing that allow the private sector to be more effective in their jobs.

The deployment of 5G technologies will enable new innovation, new markets, and economic growth around the world. Tens of billions of new devices will be connected to the Internet in the next few years. Given 5G's scope, the stakes for safeguarding our networks could not be higher. The vulnerabilities that will come with 5G deployment are broad and range from insider threats to cyber espionage and attacks from sophisticated nation-states.

Now more than ever, trust in our services and the underpinning equipment is paramount. We must realize the importance of managing risk associated with 5G deployment because there are certain areas of critical infrastructure – automated health care, telecommunications backbone, sensitive military and government facilities, and mass transit – where the scale of 5G changes the nature of risk to critical functions.

At CISA, we are committed to working with our partners and stakeholders to ensure the security and integrity of 5G technology in our nation. As we all know, adversaries are not going to stop looking for ways to attack targets of opportunity, especially those that are criticality paramount to the long-term success of our nation. Working together we will ensure a safer, more secure, and resilient tomorrow.



Christopher Krebs,
Director, Cybersecurity and Infrastructure Security Agency

WHAT IS 5G?

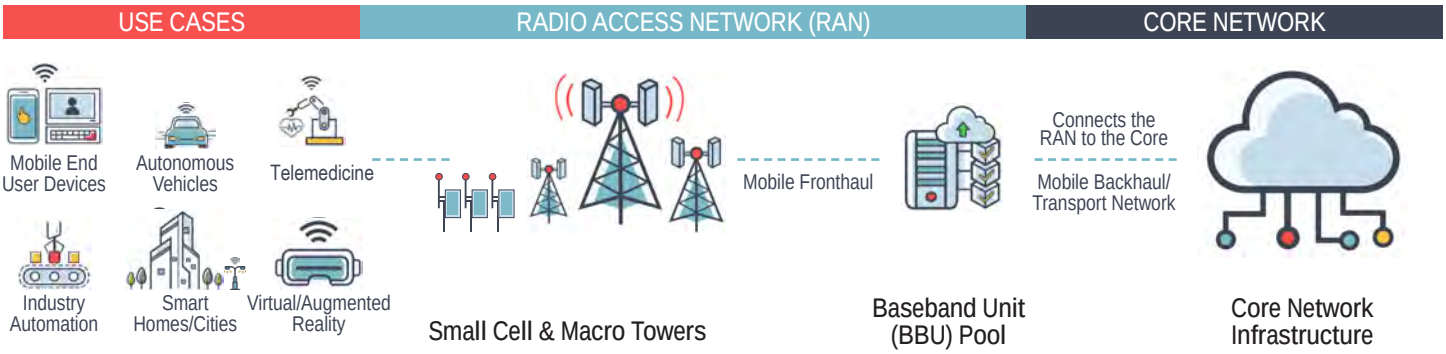
Roughly every 10 years, the next generation of mobile communication networks is released, bringing faster speeds and increased capabilities. The first-generation (1G) of wireless networks brought the very first cell phones, 2G brought improved coverage and texting, 3G introduced voice with data/internet, and 4G/4G long-term evolution (LTE) delivered increased speeds to keep up with mobile data demand. The fifth-generation (5G) of wireless technology represents a complete transformation of telecommunication networks, introducing a wealth of benefits such as higher data rates (extremely fast download speeds), ultra-low latency (near real-time interactivity), and increased network capacity (allowing for the connectivity of many more devices at once). These benefits will pave the way for new capabilities and support connectivity for applications like smart cities, autonomous vehicles, remote healthcare, and much more.

100x
Faster Download Speeds
While a 3-gigabyte movie would take 40 minutes to download on 4G, it would take only 35 seconds on a 5G network.

10x
Decrease in Latency
Data response times will be as low as 1 millisecond, providing endless possibilities from remote surgery to self driving cars.

100x
Network Capacity
5G promises greater traffic capacity, allowing for millions of devices to be connected on the same network within a small area.

Initial 5G deployment will operate on a non-standalone (NSA) network, relying on existing telecommunications infrastructure (e.g., 4G-LTE) to provide improved bandwidth, capacity, and reliability of wireless broadband services. The evolution from NSA to standalone (SA) 5G networks, which do not rely on existing infrastructure, will take years. However, the transition to a SA network will allow end-users to realize the full potential of 5G, enabling applications that require connectivity for tens of billions of devices over large areas, ultra-low latency for critical near-real time communications, and faster, more reliable connections in crowded areas. Here's how it will work:



5G networks will enable the connection for billions of new devices, sensors, and systems that will intelligently connect to the network based on their time sensitivity and computational needs.

Small Cell & Macro Towers
5G networks will leverage low-, mid-, and high-band spectrum, requiring the deployment of small cells in addition to macro towers. These small cells will serve as signal repeaters, providing improved speed, greater network capacity, and stronger reliability in high-density areas.

Baseband Unit (BBU) Pool
The centralized BBU Pool implements software-defined networking (SDN) and multi-access edge computing to allocate the network based on need and connects to remote radio units located on macro towers through mobile fronthaul (optical fiber).

Core Network Infrastructure
The core network is the backbone of the U.S. communications infrastructure that routes data and connects the different parts of the access network.

5G STRATEGIC CONTEXT

5G networks and future communications technologies (e.g., SDN, network slicing, edge computing) will transform the way we communicate, introducing a vast array of new connections, capabilities, and services. However, these developments introduce significant risks that threaten national security, economic security, and impact other national and global interests. Given these concerns, the United States and other like-minded countries have placed an increased emphasis on ensuring the security and integrity of 5G technology. For example, security officials from over 30 countries, including the United States, met in Prague in May 2019 to discuss guidelines for secure 5G network deployment. The result of the engagement was the development of *The Prague Proposals*, which identified recommendations in four distinct categories in preparation of 5G roll-out: (1) Policy, (2) Technology, (3) Economy, and (4) Security, Privacy, and Resilience.

Building upon the recommendations established by the *Prague Proposals*, the United States developed the *National Strategy to Secure 5G*, a strategic document that supports the goals of the *National Cyber Strategy* and expands on how the U.S. Government will secure 5G infrastructure domestically and abroad. The *National Strategy to Secure 5G* also identifies four major lines of effort to maximize the security of 5G infrastructure.[1]

The Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) leads 5G risk management efforts so the United States can fully benefit from all the advantages 5G connectivity promises to bring. In support of CISA's operational priority to secure 5G, as outlined in the *CISA Strategic Intent*, the *CISA 5G Strategy* establishes five strategic initiatives that stem from the four lines of effort defined in the *National Strategy to Secure 5G*. Guided by three core competencies: Risk Management, Stakeholder Engagement, and Technical Assistance, these initiatives include associated objectives to ensure there are policy, legal, security, and safety frameworks in place to fully leverage 5G technology while managing its significant risks. With the support of CISA and its partners, the *CISA 5G Strategy* seeks to advance the development and deployment of a secure and resilient 5G infrastructure, one that enables enhanced national security, technological innovation, and economic opportunity for the United States and its allied partners.

1. https://www.whitehouse.gov/wp-content/uploads/2020/03/Nation-al-Strategy-5G-Final.pdf

NATIONAL STRATEGY TO SECURE 5G

Lines of Effort:

1. Facilitate Domestic 5G Rollout
2. Assess Risks to and Identify Core Security Principles of 5G Infrastructure
3. Address Risks to United States Economic and National Security During Development and Deployment of 5G Infrastructure Worldwide
4. Promote Responsible Global Development and Deployment of 5G

OUR VISION

5G connectivity that enhances national security, technological innovation, and economic opportunity.

OUR MISSION

Lead 5G risk management efforts to promote the development and deployment of secure and resilient 5G infrastructure.

CORE COMPETENCIES

Risk Management

Promote secure and resilient 5G deployment by leading efforts to identify, analyze, prioritize, and manage risks

Stakeholder Engagement

Actively engage federal, state, local, tribal and territorial, industry, association, academia, non-profit, and international partners to address 5G challenges

Technical Assistance

Update and develop instructional tools and services to support stakeholders with the planning, governance, operational, and technical aspects of secure 5G deployment

WHO WE PARTNER WITH

CISA is committed to working with its partners to ensure secure and resilient 5G technology for the nation and its allies. As the Nation's risk advisor, CISA serves the unique role as a trusted information broker across the public and private sector. In this role, CISA fosters increased information sharing and helps stakeholders make more informed decisions when identifying and addressing future 5G technology priorities. Participation in this effort is based on a clear and shared interest in ensuring the security and resilience of the Nation's critical infrastructure and a secure and resilient deployment of 5G infrastructure.

FEDERAL DEPARTMENTS AND AGENCIES

Through information sharing and coordination with federal departments and agencies, CISA helps establish collective risk management strategies that support the development of national policy and strategy frameworks for future 5G deployment.

SLTT GOVERNMENT AGENCIES

CISA partners with state, local, tribal, and territorial government agencies to understand common vulnerabilities and share assessments of potential risks posed by 5G technology. In addition, CISA works with SLTT stakeholders to discuss the specific policy, technological, and legal implications inhibiting secure 5G deployment.

INDUSTRY

CISA relies on its partnership with the private sector to understand and manage risks posed to 5G technology. With the promise of connectivity between billions of Internet of Things (IoT) devices, it is critical that CISA and industry collaborate to identify vulnerabilities and ensure that cybersecurity is prioritized within the design and development of 5G technology.

NON-GOVERNMENTAL ORGANIZATIONS

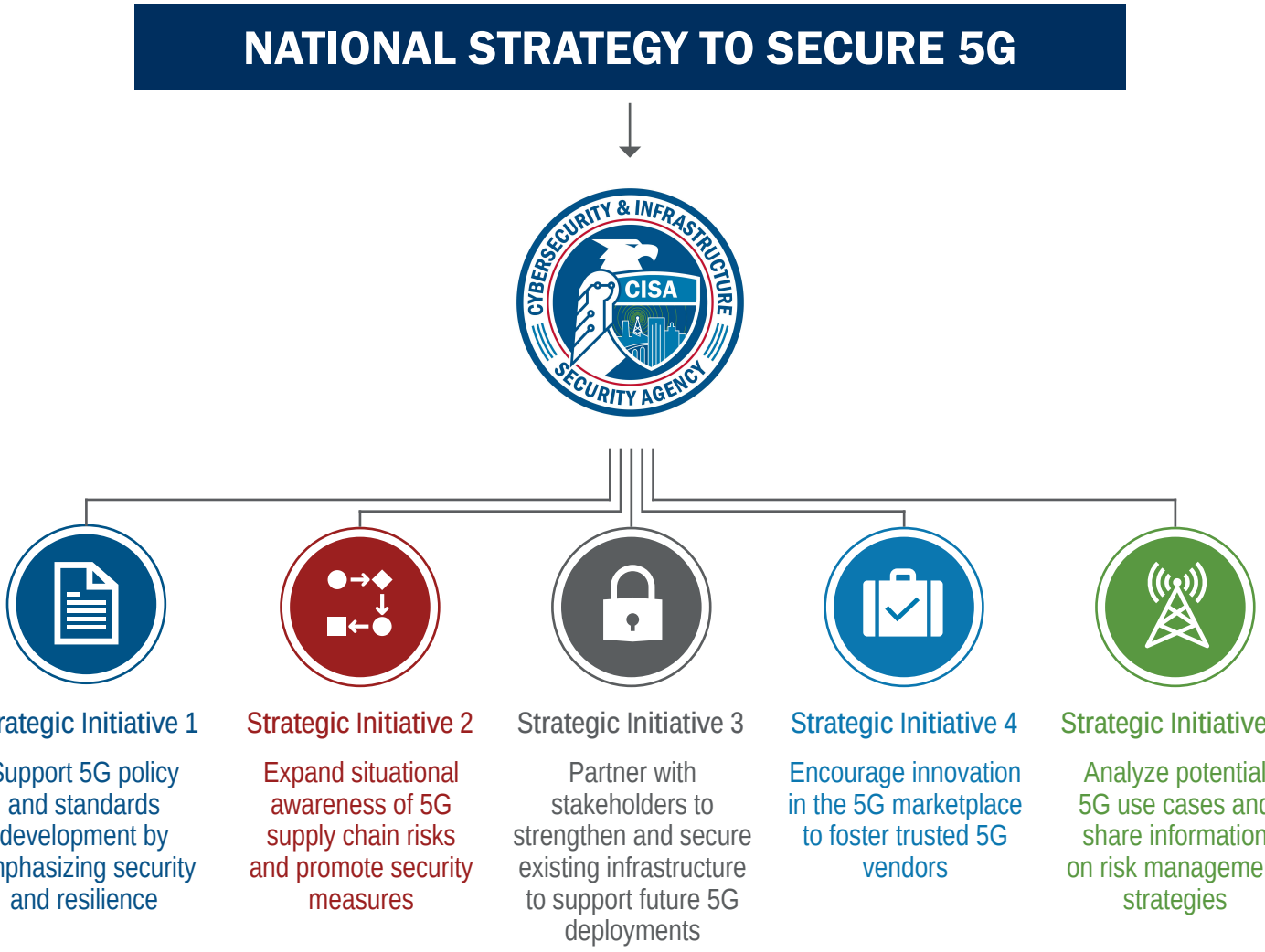
The research and development (R&D) initiatives carried out by associations, academia, and non-profits is invaluable to the security and resilience of 5G networks. From the analysis, design, testing, and development of new 5G capabilities, partnerships with these entities provide both subject matter insight and expertise that promote secure 5G deployment.

INTERNATIONAL ALLIES

As 5G connectivity becomes a reality, there is the potential for an increase in untrusted vendors, equipment, and devices. Whether vulnerabilities are malicious or inadvertent, there will remain a need to maintain strong relationships with international partners to communicate risks and safeguard the flow of information.

5G STRATEGIC INITIATIVES

The CISA 5G Strategy aligns to the *National Strategy to Secure 5G* and establishes five strategic initiatives that seek to advance the deployment of a secure and resilient 5G infrastructure. Each of the strategic initiatives address critical risks to secure 5G deployment, such as physical security concerns, attempts by threat actors to influence the design and architecture of the network, vulnerabilities within the 5G supply chain, and an increased attack surface for malicious actors to exploit weaknesses. Within each strategic initiative are objectives that define specific actions and responsibilities to ensure the security and resilience of 5G technology in our Nation.



STRATEGIC INITIATIVE 1

Strategic Initiative 1: Support 5G policy and standards development by emphasizing security and resilience

The development of 5G policies and standards serve as the foundation for securing 5G's future communications infrastructure. Those entities that shape the future of these policies and standards position themselves as global leaders and help facilitate secure deployment and commercialization of 5G technologies. To prevent attempts by threat actors to influence the design and architecture of 5G networks, it is critical that these foundational elements be designed and implemented with security and resilience from the start.

DESIRED OUTCOME: Threat actors are unable to maliciously influence the design and architecture of 5G networks.

OBJECTIVES

1.1 Expand and coordinate participation in government and industry 5G working groups and standards body meetings

CISA actively participates across numerous 5G standards bodies and working groups to bolster security and resilience, including groups like the Communications Security Reliability and Interoperability Council (CSRIC). To further their participation, CISA will continue to identify additional opportunities to provide subject matter expertise and risk management support. To ensure the distribution of streamlined and consistent messaging across all support areas, CISA will also develop an internal working group to consolidate and coordinate all efforts.

1.2 Partner with trusted market leaders to increase 5G standards contributions

The development of technical standards contributions from adversarial nations has the potential to allow untrusted technologies and equipment to capitalize on standards that are unique to their systems. The development of standards from adversarial nations is also indicative of strong influence among standards bodies, such as the 3rd Generation Partnership Project (3GPP), the leading global telecommunications standards development body. CISA will partner with trusted market leaders and other leading standards contributors like the International Telecommunication Union, Institute of Electrical and Electronics Engineers, and the Alliance for Telecommunications Industry Solutions to assist with the development of standards contributions that help eliminate vulnerabilities and the potential for corruption.

1.3 Support international 5G security and resilience policy framework development efforts

To ensure interoperable and secure communications between the U.S. and its allies, it is vital that policies are in place that promote security within 5G systems and networks. To ensure that security is a primary consideration among policy development, CISA will continue to engage with international partners and communicate the potential impacts of using untrusted 5G components and vendors, illustrating potential risks to national security and critical infrastructure.

SPOTLIGHT: CSRIC Working Groups

A key venue for collaborative work between government and the private sector is the Federal Communications Commission's (FCC) CSRIC. CSRIC is a federal advisory committee made up of members from both the private sector and government. Its mission is to provide recommendations to the FCC to ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety. As an active member of this council, CISA participates on CSRIC VII's Working Group 2: *Managing Security Risk in the Transition to 5G* and Working Group 3: *Managing Security Risk in Emerging 5G Implementations* to provide recommendations for mitigating risks and identifying best practices within the design, deployment, and operation of 5G networks.

CSRIC
Communications Security, Reliability and Interoperability Council

STRATEGIC INITIATIVE 2

Strategic Initiative 2: Expand situational awareness of 5G supply chain risks and promote security measures

Between untrusted components, vendors, equipment, and networks, 5G supply chain security is under constant threat. For example, while certain 5G equipment may be from a trusted vendor, supporting components manufactured or handled by untrusted partners or malicious actors could negate any security measures in place. These compromised components have the potential to affect the connectivity and security of transmitted data and information.

DESIRED OUTCOME: Malicious or inadvertent vulnerabilities within the 5G supply chain are successfully prevented or mitigated.

OBJECTIVES

2.1 Collaborate with Information and Communication Technology (ICT) supply chain efforts within the Federal Government to unify 5G supply chain risk management workstreams

The U.S. Government has established several supply chain security initiatives, including the formation of groups like the ICT Supply Chain Risk Management (SCRM) Task Force and Federal Acquisition Security Council (FASC). Groups like these provide complementary insights and recommendations to 5G supply chain risk management efforts. To foster increased information sharing and support additional initiatives that assess and manage risks to 5G supply chain, CISA will identify and partner with various working groups, task forces, and other supply chain-focused entities to unify efforts and workstreams.

2.2 Develop a common framework to evaluate, prioritize, and communicate 5G supply chain risks

High-risk vendors and untested components have the potential to increase the susceptibility of the 5G supply chain to unique and complex risks. Management of these risks will require timely and actionable 5G supply chain risk management information sharing. To defend against these vulnerabilities, CISA will work with the ICT SCRM Task Force, a public-private supply chain risk management partnership, to develop a framework for assessing and communicating risks. Building upon initiatives like the Task Force's development of a framework for vendors to use to attest to supply chain best practices, CISA will partner with the Task Force to define processes that prioritize supply chain risks based on their severity and impact to critical processes and functions. CISA will also work with the Task Force to disseminate valuable 5G supply chain risk management information that enables users to secure their systems, networks, and devices.

2.3 Create customized outreach materials promoting supply chain risk management strategies

To assist stakeholders with managing vulnerabilities specific to their supply chain, CISA will develop tailored outreach products that focus on risks within each of the critical infrastructure sectors. Stakeholders can leverage the information and begin to establish proactive measures and repeatable processes to manage and assess their supply chain security risks.

SPOTLIGHT: Federal Acquisition Security Council

The FASC serves as a dedicated interagency body to protect the U.S. Government's acquisition of ICTs. As a statutory member of the FASC, CISA works with other senior leaders from across the government to develop criteria and information sharing that assists departments and agencies with identifying and managing specific ICT supply chain risks, including those risks posed to 5G technologies. The FASC also reviews DHS's ICT SCRM Task Force's findings and recommendations to assist with its efforts to implement the *Federal Acquisition Supply Chain Security Act*. A key component of the FASC is the ability to recommend exclusion of certain vendors or removal of certain products, subject to judicial review, to mitigate security concerns. This ability will become increasingly important as development and deployment of 5G infrastructure begins to take shape.

STRATEGIC INITIATIVE 3

Strategic Initiative 3: Partner with stakeholders to strengthen and secure existing infrastructure to support future 5G deployments

Before moving to a standalone infrastructure, the first iterations of 5G deployment will work alongside existing 4G LTE infrastructure and core networks. While 5G architecture is designed to be more secure, 5G's specifications and protocols stem from previous networks, which contain legacy vulnerabilities. For example, the overlay of 4G and 5G networks has the potential for a malicious actor to carry out a downgrade attack, where they could force a user on a 5G network to use 4G in order to exploit known vulnerabilities against them. These inherent vulnerabilities, along with new and unidentified risks, will require the collaboration of industry and government to develop and communicate security enhancements to support secure 5G deployments.

DESIRED OUTCOME: Secure 5G deployment, void of legacy vulnerabilities and untrusted components.

OBJECTIVES

3.1 Collaborate with national laboratory and technology centers to evaluate key existing 5G components and identify security vulnerabilities

5G will use more components than previous generations of networks, and the proliferation of 5G infrastructure could provide malicious actors with more attack vectors. To counteract these risks, CISA will collaborate with academia, national laboratories, and technology centers, like the Idaho National Laboratory, to establish testing programs that address 5G security and vulnerability challenges associated with 5G handsets, radio access networks, and other 5G components.

3.2 Direct engagements to promote security and resilience of 5G deployment across the critical infrastructure sector and SLTT communities

As 5G networks are deployed among the critical infrastructure sectors and SLTT communities, CISA will lead engagements to communicate known risks and best practices that support secure and resilient 5G. These engagements will include the facilitation and coordination of outreach through meetings, workshops, conferences, and other events.

3.3 Coordinate across the Federal Government to engage with international partners and promote 5G deployment best practices

Sharing information and promoting security best practices among international partners is critical to establishing secure and interoperable 5G communication among the United States and its allies. To ensure a consolidated and coordinated effort when engaging international partners, CISA will leverage its federal partnerships to develop and promote best practices that help identify standards for procuring trusted 5G technology and establish information-sharing mechanisms that educate stakeholders on new and emerging 5G vulnerabilities.

SPOTLIGHT: Rural Engagement Initiative

The Rural Engagement Initiative leverages CISA's partnerships across the Federal Government and rural telecommunications carriers in a collaborative effort to discuss 5G innovation, security, and risk mitigation efforts. This effort brings together DHS, the FCC, the U.S. Chamber of Commerce, the Competitive Carriers Association, and small owner/operators from across the Nation. Engagements will provide an interactive forum for round table sessions and discussions on the future of 5G.

STRATEGIC INITIATIVE 4

Strategic Initiative 4: Encourage innovation in the 5G marketplace to foster trusted 5G vendors

As 5G is deployed, there is an emphasis on ensuring that state-influenced entities do not dominate the 5G marketplace. To address this concern, CISA will work with its partners to support R&D initiatives and prize programs that result in secure and resilient 5G technologies and capabilities. By supporting these types of efforts, CISA will help drive innovation and establish a trusted vendor community for the future of 5G.

DESIRED OUTCOME: Increased number of trusted vendors in the 5G marketplace to address risks posed by limited competition and proprietary solutions.

OBJECTIVES

4.1 Collaborate with federal interagency partners to establish R&D projects focused on emerging 5G technologies and capabilities

To assist with managing the risks associated with 5G technologies and its new capabilities, CISA will work with its federal interagency partners to coordinate, identify, develop, or adapt R&D efforts (e.g., Open RAN, network slicing, and intrusion detection and prevention systems) to meet 5G strategic needs. These efforts will result in tools, technologies, and informational products that will help bridge the gap between industry and its end-user communities, providing stakeholders with a greater understanding of how to securely deploy 5G infrastructure and technology and leverage all the benefits its connectivity promises to bring.

4.2 Analyze and report the long-term risks of untrusted 5G component vendors

Procurement of 5G components from untrusted vendors poses many economic and security risks. Often, these technologies are cheaper than trusted alternatives, but these low, up-front costs have the potential to accumulate into more long-term expenditures to address security flaws or interoperability issues. To prevent the United States and its allies from purchasing untrusted equipment, CISA will analyze components from 5G vendors and report on any long-term risks that affect the ability to securely communicate and share information.

4.3 Partner with U.S. Government (USG) prize competition programs to influence and establish 5G innovation challenges

USG prize competitions serve as programs that stimulate innovation and seek to identify or develop solutions that have the potential to advance the mission of a federal agency. As part of CISA's mission to manage risk to the Nation's critical infrastructure, CISA will partner with USG prize competition and innovation challenge programs (e.g., DHS InnoPrize Program) to encourage the facilitation of projects that promote the development of secure and resilient 5G technology and infrastructure.

SPOTLIGHT: BAA Issued between CISA and DHS S&T

The Broad Agency Announcement (BAA) solicitation, published in April 2019 between CISA and the Science and Technology Directorate (S&T), established an R&D project for a Secure and Resilient Mobile Network Infrastructure (SRMNI). The project seeks innovative approaches and technologies to protect legacy, current, and 5G mobile network communications, services, and equipment against all threats and vulnerabilities.

> "The deployment of 5G technologies offers opportunities for innovation, efficiency, and economic growth, but it may also present risks we're not currently positioned to manage… This BAA solicitation and SRMNI R&D will help DHS work with industry to identify threats and vulnerabilities to mobile network infrastructure and inform the development and adoption of security standards."
>
> **Christopher Krebs**
> **Director, Cybersecurity and Infrastructure Security Agency**

STRATEGIC INITIATIVE 5

Strategic Initiative 5: Analyze potential 5G use cases and share information on identified risk management strategies

The enhanced capabilities of 5G technologies will support an array of new functions and devices, introducing a plethora of potential use cases. With the potential for the connection of billions of devices on a network, also known as massive Machine-Type Communication (mMTC), applications like smart cities will require increased security to safeguard connected devices from potential threats and vulnerabilities. To ensure the security and integrity of these devices, CISA will communicate known vulnerabilities and risk management strategies for use cases associated with securing the Nation's critical functions.

DESIRED OUTCOME: New vulnerabilities introduced by deployments of 5G technology are clearly understood and managed.

OBJECTIVES

5.1 Identify, prioritize, and evaluate potential 5G use cases in real and simulated environments

Development of risk management strategies requires the assessment of future 5G use cases. Through real and simulated environments, CISA will identify and prioritize 5G use cases that are so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Results from these assessments will influence the development and dissemination of risk management strategies.

5.2 Develop and deliver 5G technical assistance offerings to address stakeholder specific use cases

Leveraging results from 5G use case evaluations, CISA will develop and deliver customized 5G technical assistance offerings, consisting of trainings, tools, and onsite assistance, that cater to a stakeholder's specific needs. These technical assistance offerings will help stakeholders prepare and plan for the deployment of 5G infrastructure, navigate the complexity of 5G technologies, and secure communications and data transmitted through 5G networks.

5.3 Leverage industry expertise and analysis to develop informational materials promoting security best practices for 5G enabled IoT devices

5G networks will enable the expansion for billions of IoT devices, supporting the advancement of industrial control systems and industries like smart cities, health care, transportation, public safety, agriculture, and industrial automation. While these innovations provide a wealth of new capabilities, they also introduce the potential for increased attack vectors for malicious actors to expose. Building upon the initial 5G risk characterization initiative, CISA will leverage industry expertise and analyses to develop risk management insights that promote secure product design and inform the end-user of cybersecurity best practices.

SPOTLIGHT: 5G Use Cases

As identified by 3GPP, initial 5G applications will be organized by use case type, which are defined by their unique characteristics and services they facilitate.

Use Case Type	Characteristics	Sample Applications
eMBB Enhanced Mobile Broadband	Enhanced mobile broadband uses high-band spectrum and provides a greater capacity to support high data rates providing consumers with a faster, more reliable connection in crowded areas and on the move; but due to the non-penetrative signal and short range, increased infrastructure will be required.	Augmented/Virtual Reality; Work/Play in the Cloud; Mobile Ultra High-Definition (UHD, 4K, 8K); Smart Home
URLLC Ultra Reliable Low Latency Communication	Leveraging mid-band spectrum, Ultra Reliable Low Latency Communication can cover large areas (several miles) and serves applications that require high reliability and are extremely sensitive to latency, often for mission-critical applications.	Autonomous Vehicles; Remote Medical Procedures; Industry Automation; Public Safety
mMTC Massive Machine-Type Communication	Massive Machine-Type Communication provides connectivity to billions of devices that transmit small amounts of traffic intermittently through low-band spectrum that can cover very large areas (hundreds of miles). These applications are not highly dependent on latency.	Smart Cities; Remote Healthcare; Transport and Logistics; Intelligent Agriculture

CONCLUSION

The transition to 5G presents a wealth of opportunities and new capabilities, changing the way the world communicates and shares information. With increased capabilities like faster download speeds and ultra-reliable connectivity, 5G networks will spark an industrial revolution that will enable the development of many new and enhanced services like autonomous vehicles, smart cities, augmented reality, and remote surgery. Given the potential for various applications and reliance of the network for future infrastructure, the stakes for safeguarding the network against these vulnerabilities could not be higher.

The use of established critical infrastructure sector partnerships will be one of the backbones of CISA's efforts within 5G, as the nature of the risk environment precludes any single entity from managing risk entirely on its own. As the Nation's risk advisor, CISA is committed to working with its partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. Moving forward, CISA will leverage its partnerships with SLTT, industry, association, academia, non-profit, and international allies to implement the five strategic initiatives and 15 objectives defined in this plan. Only by working together will CISA realize the vision of the CISA 5G Strategy: *"5G connectivity that enhances national security, technological innovation, and economic opportunity."*

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency