NYC Cyber Command

NYC Mayor's Office of the Chief Technology Officer

June 25, 2020

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

RE: The National Strategy to Secure 5G Implementation Plan
[Docket No. 200521–0144; RIN 0660–XC047]

The City of New York (City) appreciates the opportunity to comment on the development of an Implementation Plan for the National Strategy to Secure 5G. The following comments are based on New York City's own implementation plan (the NYC Internet Master Plan), released in January 2020, and the efforts of NYC Cyber Command (NYC3) to ensure strong cybersecurity practices for current and new technologies used by and within the city.

Affordable, reliable, and equitably distributed high-speed internet access is critical to the economic and personal well-being of the city's nearly 8.4 million residents. Currently, broadband services available from private companies continue to leave behind too many New Yorkers. While a majority of New Yorkers do have access to broadband, more than 1.5 million residents still have neither a connection at home nor on a mobile device.

Our city is committed to fighting income inequality and ensuring all New Yorkers have opportunities to succeed. That means every New Yorker should have affordable and reliable access to high-speed broadband so that they have access to quality educational opportunities, health care, and essential services. As the recent COVID-19 pandemic has laid bare, access to reliable broadband is now a prerequisite, similar to a public utility, to ensure personal safety, education, and opportunities for economic growth for New Yorkers.

As outlined in the NYC Internet Master Plan, 5G technology is uniquely well-suited to a dense urban environment such as New York and we recognize the importance of ensuring that 5G is deployed in a manner that contributes to closing the digital divide, not widening it.

While this new technology brings the potential for great opportunity, its deployment brings new risks and national security concerns. As a center of commerce with a gross domestic product that rivals many nations, New York City is a target for economic espionage by foreign governments. Our city is home to some of the largest corporations in the United States, as well as an innovative and thriving startup culture. Emerging technologies built in New York City drive over $70 billion in startup valuation and exits each year. 5G represents a new threat vector for nation-states and other foreign actors intent on stealing intellectual capital from our residents.

Beyond economic interests, there are political and cultural reasons our city is a high-profile target for adversaries that seek to undermine the integrity of our infrastructure for other nefarious purposes.

Technology components critical to the rollout of 5G in the U.S. will almost certainly require significant (if not critical) reliance on foreign technology firms, manufacturers, and their supply chain ecosystems—particularly China, who has historically sought to "access information about U.S. firms' proprietary operations and project-financing information, as well as steal IP and technology" through cyber espionage, according to the U.S.-China Economic and Security Review Commission. This creates a significant supply chain risk.

New York City is highly concerned about the threats created by a lack of coherent national vision and strategy for securing our nation's telecommunications infrastructure. This lack of federal leadership domestically and in coordination with allies internationally makes our city vulnerable to foreign adversaries who may seek to undermine us.

For these reasons, we urge you to consider: 1) funding for state and local testbeds, development, security controls and other factors necessary in furtherance of a secure 5G deployment; 2) national authorities and standards for rigorous, ongoing testing to secure 5G technology components, as well as the devices that utilize 5G networks; 3) federal regulatory structures that provide safeguards against the risk of the increased attack surface that is likely to arise along with mature 5G network development; and, 4) engagement with key international allies on this critical national security issue.

Line of Effort 1: Facilitating Domestic Rollout

To facilitate the domestic rollout of 5G technologies and the development of a robust domestic 5G commercial ecosystem (e.g., equipment manufacturers, chip manufacturers, software developers, cloud providers, system integrators, network providers), the City urges the federal government to consider and address security-related supply chain concerns. The City is troubled by disruptions to the 5G ecosystem that are likely to increase the cost and reduce the efficiency of any 5G technology deployment, but may prove necessary to curtail systemic security concerns. Private and public investment will be vital to ensuring affordable, reliable high-speed access is available across the five boroughs of our city, ensuring all New Yorkers have access to the economic, social, and civic power of the internet.

The City recognizes the critical role that advanced technologies play in national security. Investment in the research, development, testing, and evaluation of new technologies and architectures can launch mutually-beneficial public and private partnerships through federally-funded research projects. In the near term, New York recommends federal funding for local municipal investment in secure 5G network infrastructure in an effort to promote specific security requirements around 5G network equipment and infrastructure. We will discuss more about mitigating the significant equipment-related security concerns in our response to other Lines of Effort.

The City also invites meaningful research partnerships given that we maintain one of the most appropriate environments for 5G technologies. For instance, with funding from the National Science Foundation Platforms for Advanced Wireless Research and through partnerships with academic researchers and industry stakeholders, a wireless testbed in Upper Manhattan, named COSMOS, serves as a real-world research hub for new wireless technologies and applications in one of the most populated urban environments in the world. These kinds of testbeds are necessary to ensure the appropriate scientific and technical knowledge is developed to advance new and more secure products to the market that work in many environments, including environments like New York City that require consideration of security factors unique to densely populated and urban areas.

In addition, to increase domestic 5G research, development, and testing, New York City would invite an opportunity to serve as the site for an “X-Prize” or DARPA grand challenge-style scientific innovation investment opportunity that looks to foster a secure, domestically produced 5G commercial ecosystem. This would mirror other investment approaches that have brought the United States to the forefront of ingenuity and production in certain industries—perhaps most notably in the areas of autonomous vehicles and private sector spaceflight—with investments from public and private sector entities. New York City has served as host to federal pilots and partnerships to promote telecommunications technology, including our joint effort to improve the safety of travelers and pedestrians through the deployment of Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) connected vehicle technologies. We look forward to welcoming such innovation again.

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

5G’s potential for higher speeds and other advantages also brings system complexities that may not have existed in previous generations of broadband technologies. The dynamics of 5G make this technology much less like a traditional telecommunications platform and more like the multi-layered open environment we find on the internet. Such complex systems present more opportunities for security and privacy breaches. By moving away from firmware-based technology of 4G telecommunication components to software-based 5G telecommunication components that will need to be updated, the opportunity for manipulation exists within the supply chain. Furthermore, movement away from centralized network systems to decentralized network systems increases the attack surface of a network. That increased attack surface is amplified by the anticipated introduction of the increasing number and variety of connected devices (IoT) and big data industries.

Core security principles for 5G should be built upon existing foundational security principles and programs. For example, federal standards for supply chain risk analysis have been built by the National Institute for Standards and Technology (NIST), which should be highly leveraged on the federal level and made mandatory for access to grants for deploying new telecommunications platforms, such as the ones we discussed in Line of Effort One. It should also be foundational to federal investment in the technology more generally.

New York City Cyber Command has built an Internet of Things (IoT) Lab to rigorously test publicly-owned connected devices prior to citywide deployment. Our work confirms what is well known and evident: the risk inherent in these lightweight technologies. IoT risk profiles change with their environment and specific use case, and security has generally not been the primary focus of manufacturers of these technologies. We have identified dozens of critical and high risk vulnerabilities within proposed devices. Many have already been deployed elsewhere in the country and world prior to New York City's review. New York City Cyber Command has also identified "zero-day" (previously unknown) exploits that now have published common vulnerabilities and exposures (CVEs) associated with them. These vulnerabilities have been resolved by the vendors prior to deployment in our municipality, and ultimately benefits the public and private sector by improving security.

The problem of IoT vulnerabilities will only become exacerbated by the increased speeds of 5G and other future wireless broadband technologies.

Similarly, several significant vulnerabilities have been discovered by security researchers during initial 5G rollouts in test markets. As with any new technology, it is likely that additional, potentially critical, zero-day vulnerabilities exist within 5G technology components.

We recommend the federal government provide grants to localities and states for rigorous security testing of critical devices being considered for adoption by the public sector and critical infrastructure partners. This becomes vital with the anticipated expansion of IoT device use commensurate with the increased load and speed capabilities of 5G networks.

Additionally, New York City recommends federal testing and security requirements for consumer grade IoT devices. IoT protection is historically poor and malware distribution is easily scalable, which suggests that the creation of IoT botnets ("robot networks") for malicious purposes, including large-scale distributed denial of service (DDoS) attacks, is likely to increase as well. This poses a significant threat to vital digital infrastructure and resident services at all levels of government, as well as private sector enterprise.

New York City has dedicated itself to supporting our residents' secure connectivity as the cyber threat environment has continues to escalate. New York City Cyber Command, created in 2017, is charged with securing our public infrastructure and supporting the digital security of New Yorkers. New York City Cyber Command has built security-driven solutions into public Wi-Fi connectivity points and offers our residents mobile threat protection through NYC Secure, the first-of-its-kind free mobile security application from a public entity. In addition, the City has proposed baseline and additional security standards for a higher-level of service for users of public Wi-Fi on city streets in its Truth in Broadband: Public Wi-Fi in New York City report. Such consumer-facing initiatives at the local level should be supported through federal funding to identify and raise best practices for raising cybersecurity support for the general public to meet the accelerating threat environment.

Finally, the federal government should require regular independent testing and certification of 5G telecommunication components. This testing will need to occur on a regular basis to ensure changing software does not create new vulnerabilities, and build processes for resolution when security concerns are identified.

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

The passage of the Secure 5G and Beyond Act of 2020 by Congress is just one step in addressing the risks to economic and national security in the development and deployment of 5G infrastructure. We believe a lack of national strategy leads to inconsistent international engagement around our telecommunications infrastructure. While there have been specific instances where the federal government has pushed allies away from equipment associated with foreign adversaries, such activity is not a substitute for a proactive and comprehensive approach to a complex technology market. This dynamic creates a significant security risk to our city's critical infrastructure, as well as to the privacy and economic security of our residents.

In essence, New York City is executing on our security strategy in absence of the perspective of a comprehensive federal framework. While there is no scenario where governments lead the development and deployment of 5G and future telecommunications technologies, the public sector must play a critical role in its development and deployment. From international coordination among allies, to national leadership in the executive branch, to support for state and local deployment strategies, the required federal orchestration and influence has been largely absent.

The City shares the concerns outlined in the U.S. Senate Committee on Homeland Security and Governmental Affairs Permanent Subcommittee on Investigations staff report released earlier this month that pointed to a lack of authority and process at the federal level as key factors which undermine a cohesive telecommunications review of foreign actors, endangering our national security.

New York City urges the federal government to coordinate investment from federal and private sources into research and development of domestic telecommunications technologies at public and private institutions, while creating a coordinated effort among allied countries to do the same. Beyond attempting to gain primacy in domestic 5G manufacturing, efforts should be focused on accelerating the timeline and early production of other domestically nurtured next-generation telecommunication "6G" technologies in concert with key allied nations. The City also encourages the federal government to promote 5G vendor diversity and foster market competition, so long as these actions do not negatively impact or otherwise disrupt paramount security considerations and initiatives.

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

An effective policy and regulatory framework which outlines equitable standards, incentives, and sufficient enforcement mechanisms is essential for promoting and facilitating global development and deployment of 5G. However, this framework should prioritize and support—not displace or disrupt—5G deployment and implementation initiatives at the state and local levels that provide for necessary security protections and public services that benefit city residents and businesses.

Continued disagreements and disarray among federal actors and telecommunications sector stakeholders on issues ranging from infrastructure security and supporting state and local broadband deployment efforts to confronting foreign disinformation campaigns focused on undermining our democracy is ultimately allowing foreign governments to fill the void and set standards for security and privacy in the global tech industry. Widening the gap further are federal actions that favor large telecommunications companies at the expense of consumers and local governments, including the elimination of privacy protections, affordability programs and net neutrality requirements. We can only succeed through communicating American values of inclusiveness and digital rights nationally, promoting those values internationally through strong alliances with international partners, such as New York City's participation in Cities for Digital Rights, and ultimately constructing a common vision built upon mutual security.

To promote responsible global development and deployment of 5G, the federal government must stand up for our values by: 1) not impeding the abilities of states and localities to take necessary and appropriate actions, such as those discussed in the New York City Internet Master Plan, that promote and facilitate broadband services and enable affordable, equitable, reliable, secure high-speed broadband deployments within their communities; 2) providing funding, necessary authorization, and guidance to federal agencies tasked with monitoring foreign manufacturers and telecommunications carriers; and, 3) focusing on engaging our international allies to build standards that provide mutual security assurances.

Thank you for your dedication to this issue. We stand ready to work with our federal partners to secure our nation's vital telecommunications infrastructure and ensure the availability of secure high-speed, reliable, quality broadband service for all New Yorkers.

Sincerely,

John Paul Farmer

Geoff Brown

Chief Information Security Officer
City of New York

John Paul Farmer

Chief Technology Officer
City of New York