Written Comment for the National Telecommunications and Information Administration Implementation Plan for the National Strategy to Secure 5G.
Docket No. 200521-0144

James A. Lewis, SVP and Director, Center for Strategic and International Studies
June 17, 2020

As part of its work on an Implementation Plan for the National Strategy to Secure 5G, mandated by the Secure 5G and Beyond Act of 2020, the National Telecommunications and Information Administration (NTIA) has requested comments on Executive Branch efforts for the development of a strategy to ensure the security of next generation wireless communications systems and infrastructure. CSIS appreciates the opportunity to submit this short note touching on key issues.

A strategy must be based on a realistic assessment of U.S. strengths. The United States is not losing the 5G "race." American (and Japanese) technologies are essential for 5G infrastructure; America is holding its own in the standards bodies and is well placed to repeat the commercial success it had with 4G. The telecom supply chain depends on semiconductors and software, all areas where the U.S. has a substantial lead. The problems attributed to a 5G "race" are overstated, but the United States would benefit from policies to speed deployment, reduce supply chain risk, ease technological transition, and increase economic opportunities.

5G technologies meet the growing demand to move data and knowledge faster, more reliably, and more efficiently. 5G creates wealth by enabling new "enterprise" services for industry and by building the network that will support the Internet of Things. The "killer apps" for 5G have not yet been developed, but this will change as entrepreneurs explore newly available 5G capabilities and develop services and products to use it.

A national strategy should address four issues: accelerating deployment and spectrum reallocation, building a diverse and trustworthy supply chain and a competitive international marketplace for 5G technologies, ensuring international cooperation with governments and companies (which is the key to success in standards bodies and to maintaining a flourishing competitive environment), and managing technological transition to next generation telecom network technologies. The elements of a comprehensive approach should include:

- **Emphasizing American technological competitiveness**. This means not only expanding Federal support for research but also looking at intellectual property law, anti-trust, taxation, and spectrum allocation to optimize them for innovation.

- **Reprioritizing spectrum allocation**. NTIA and the FCC have done a good job in supporting 5G deployment, but the United States risks finding itself at a disadvantage in 5G deployments because of spectrum allocation decisions made years or even decades ago, particularly in regard to mid-band spectrum. While spectrum decisions have not yet put the United States at a competitive disadvantage, the issue in spectrum allocation is one with which NTIA is familiar:, the process for deciding when the Department of Defense and other Federal agencies should retain spectrum or when spectrum should be reallocated to commercial purposes could lead to competitive disadvantage.

- **Supporting government users affected by changes in spectrum policy**. Access to mid-band spectrum may require moving incumbent users or subsidizing their acquisition of new equipment that reduces the risk of interference. In a previous case during the Bush Administration, this involved auctioning off spectrum and then using the funds produced by auction to compensate Federal agencies (working with the Office of Management and Budget to ensure that the new funds were considered as an addition to existing agency budget allocations and not as a replacement). Given the changing nature of international competition, where commercial innovation is more important to American interests and to national security, reprioritizing spectrum use is in the national interest.

- **Encouraging 5G deployment**. Deployment issues include, in addition to spectrum reallocation, encouraging local governments to speed the approval of 5G infrastructure. Given the division of responsibilities in a Federal system, this issue must balance local concerns with the national interest in rapid 5G deployment. As experience grows with the deployment of 5G cell towers, local concerns may be mitigated by informational efforts by NTIA, FCC and others to provide a better public understanding of opportunities and solutions that have worked elsewhere.

- **Increasing support for research and development**. The goal of R&D should be to preserve diversity in telecommunications technology suppliers so that we do not find ourselves dependent on suppliers from a hostile country. It should also include research into developing the next generation of telecommunications equipment, and the secure use of 5G networks.

- **Researching how to securely communicate over untrustworthy international networks**. Finding ways to mitigate the security risks of untrusted networks will be essential, since many European, African and Middle Eastern companies already use less trustworthy network technologies.

- **Supporting the semiconductor industry**. A 5G strategy should support the American semiconductor industry by developing policies for research, education, and intellectual property protection, and by pushing back against foreign efforts to hobble U.S. competition. Software and semiconductors will form the basis of the next generation of telecommunications infrastructure and the U.S. faces increased competition, particularly in semiconductors, that requires a response. The CHIPS for America Act recently introduced by Senators Cornyn and Warner makes a valuable contribution n this regard, given the importance of semiconductors for telecommunications technology.

- **Promoting international measures to avoid dominance by single suppliers**. A package of international measures—such as reliable standards, trustworthiness and security principles, and foreign assistance to counter Chinese subsidies—offer the best opportunity to avoid a global telecommunications network dominated by a single company. The United States and like-minded countries should provide foreign assistance funding to encourage developing countries to rely on a diverse and trustworthy telecom supplier base. The U.S should strengthen partnerships to ensure that the standards making

process for 5G remains fair and that decisions are based on technological rather than political considerations.

- **Adopting robust security standards and trustworthiness criteria for telecommunications equipment and supply chains**. The Prague Proposal and the EU 5G Tool Box offer good starting points for this. Working with a group of Asian, American and European private sector experts, CSIS developed the attached non-technical criteria for identifying trustworthy suppliers (also available at www.csis.org/analysis/criteria-security-and-trust-telecommunications-networks-and-services). These Criteria for Security and Trust in Telecommunications Networks and Services can reinforce the Prague Proposal and EU Tool Box. Since some of our allies will adopt the core/edge bifurcation in telecom infrastructure in an effort to improve security, the U.S. should help them make this as effective as possible.

A number of CSIS publications discuss these ideas in detail. They include How 5G Will Share Innovation and Security, China's Pursuit of Semiconductor Independence, and Can Telephones Race? The U.S. is doing well in the deployment of 5G, but success is not guaranteed without further action and in this, NTIA's efforts at developing a national strategy are invaluable.

Attachment: Criteria for Security and Trust in Telecommunications Networks and Services

At the request of the Department of State, CSIS assembled a group of experts[i] from Asian, European and American companies and research centers to develop criteria to assess the trustworthiness of telecommunications equipment suppliers. These criteria complement the work of the Prague Proposal and the European Union's 5G Toolbox. They offer governments' and network owners or operators an additional tool to use to determine trustworthiness and security.

Communication technologies are transforming the way we live and work. These changes create risks as well as opportunity, since the rapid development and scale of communication technologies can increase dependency and vulnerability. The global supply chains used for telecommunications networks' software and hardware can raise security concerns, including increasing concern about the risks posed by the acquisition and deployment of communications technologies from untrustworthy suppliers. One key issue facing nations is how to assess the trustworthiness and security of technologies provided by different suppliers. Given their sensitivity for national security, telecommunications systems should only be sourced from trustworthy suppliers or manufacturers.

Bearing this in mind, and building on the work of the Prague Proposal and the European Union's 5G Toolbox, we have developed the following criteria for governments and network owners or operators to use in a comprehensive and objective fashion to determine trustworthiness and security. These criteria rely primarily on publicly available information to allow for an assessment of the trustworthiness and security of a potential supplier, and to describe domestic policies to guide responsible and necessary actions to safeguard telecommunications networks. These criteria are derived from different assessment tools, such as foreign investment screening, national security reviews, and commercial practices and allow for fact-based decisions on how trustworthy a supplier is likely to be. Governments can apply these criteria equally and transparently in a cumulative fashion to all companies to assess risk and security.

Political and Governance Criteria

1. Suppliers are more trustworthy if they are headquartered in countries (and hence subject to national laws and other governmental actions) with democratically elected governments, as evidenced by the presence of viable and independent opposition parties, elections where the incumbent administration can be or has been displaced, and a separation of powers between judicial, legislative, and executive functions.

2. Suppliers are more trustworthy if they are headquartered in a country with an independent judiciary, as evidenced by a record of actions that indicate respect for principles such as presumption of innocence and the right to a public hearing, the right to be tried without undue delay, and the existence of courts or tribunals that follow established procedures and legal processes without being subject to political interference.

3. Suppliers are more trustworthy if they are headquartered in a country where the laws and policies governing networks and connectivity services are guided by a demonstrable

respect for the rule of law, shown by clear legal or judicial limitations on the exercise of power by the government where there is evidence that these limitations have had effect.

4. Suppliers are more trustworthy if they are headquartered in nations that are security partners with the government of an acquirer or where there are cooperative security arrangements between the government of an acquirer and the government of the supplier.

5. Suppliers are more trustworthy if they are headquartered in countries with a demonstrable record of protecting personal data, as evidenced by multilateral agreements, law, and regulation, enforcement actions, or adequacy decisions on data protection by an independent authority.

6. Suppliers are more trustworthy if they are headquartered in countries with a demonstrable record of observance of their international human rights commitments, including a demonstrably free media and an absence of censorship, arbitrary detentions, or other actions contrary to accepted human rights practices and international norms.

7. Suppliers are more trustworthy if they are selected as the result of an acquisitions process based on factors other than only cost, taking into account labor conditions, trade practices, human rights, and environmental standards.

8. Suppliers are less trustworthy if they exhibit a pattern of behavior and practices outside widely accepted international commercial norms that indicate interdependence between a company and a host government. The criteria for assessing this include, for example, legal or formal requirements that government or political party representatives be part of a supplier's administration or management, have arbitrary access to company data and operations, or can compel cooperation or impose obligations for intelligence purposes on the company without it having the right to appeal to an independent judiciary.

9. Suppliers are less trustworthy if the national laws of the country where they are headquartered mandate cooperation with the government or give the government special rights that cannot be challenged in court or the national legislature.

10. Suppliers are less trustworthy if they or their host governments have a record of engaging in predatory trade practices (such as "dumping," unconditional state subsidies, or the use of artificially low prices) or other practices intended to provide unfair advantage.

Business Practices Assessment Criteria

11. Suppliers are more trustworthy if they have transparent ownership and corporate governance structures that can be independently verified.

12. Suppliers are more trustworthy if they are publicly traded or otherwise subject to regulatory requirements that require disclosure or enable examination of the company.

13. Suppliers are more trustworthy if they are financed openly and transparently, use best

practices in procurement, investment, and contracting, and have records available for public or regulatory scrutiny as appropriate.

14. Suppliers are more trustworthy if they can demonstrate adherence and observation of internationally recognized accounting standards (such as the Generally Accepted Accounting Principles or the International Financial Reporting Standards).

15. Suppliers are more trustworthy if they have a history of due diligence and ethical corporate behavior, including respect for the intellectual property of others.

16. Suppliers with opaque ownership structures, which are state-owned, or where ownership is restricted to nationals of a single country are less trustworthy. Opaqueness is indicated by unusual ownership arrangements that disguise who owns, controls, or influences the supplier company or use any other mechanisms to conceal dependencies between the supplier and a foreign state.

17. Suppliers are less trustworthy if they benefit from hidden or opaque financial support or incentives, subsidies, or other financing mechanisms that are not commercially reasonable; lack transparency; are part of a larger effort involving predatory pricing intended to eliminate competition; force other suppliers from the market; or are part of other government actions intended to disadvantage competitors unfairly.

Cybersecurity Risk Mitigation Criteria

To the extent that a supplier does not meet the trustworthiness criteria above but a government or operator decides to permit a limited deployment of that supplier's equipment despite the lack of trustworthiness, the risk of using its technology can be partially mitigated and the cybersecurity of the network increased if:

18. The supplier has successfully passed independent and credible third-party assessments, credible national risk assessments, or security evaluation processes of technical and non-technical aspects (such as the legal and policy framework to which the supplier may be subject) of its telecommunications infrastructure technology.

19. An acquiring nation or third-party assessment or certification can confirm that the assessed technology is actually deployed in the products used.

20. The supplier's products and services technology are designed, built, and maintained according to internationally recognized, open, and consensus-based standards for telecommunications technologies.

21. The supplier is able to provide assurances on the pedigree of components and software and has policies and procedures to address security and intellectual property requirements that apply to "open-source" code incorporated in or used to derive any deliverable provided to customers.

22. The supplier follows relevant commercial and technical practices for transparency of maintenance, updates, and remediation of products and services.

23. The supplier has a record of addressing and remediating security flaws identified by customers in a reasonable period of time.

24. The supplier provides operational support in ways that are consistent with the national cybersecurity policies and rules to which the operator is subject and maintains information security governance policies that conform to applicable data protection laws and requirements and verifiably address such requirements.

25. The supplier is able to demonstrate that it has adequate oversight and contractually binding security and quality assurances with third-party providers of components for its products.

26. The supplier follows secure development practices and is able to document adequate lifecycle management for software tools and source code.

27. The supplier has implemented verifiable technical measures to ensure the application of strict access controls (that limit access to authorized users, authorized processes acting on behalf of authorized users, or authorized devices) and security monitoring for the supported network that are consistent with the network operator's security policies.

Government Actions to Increase Confidence in Choosing a Supplier

28. Governments should have the policy and legal tools to assess a supplier's risk profile and determine that suppliers are able to demonstrate trustworthiness based on both independent assessments and assessments that apply non-technical criteria identified above. Suppliers should be able to demonstrate that they use secure design, software engineering, and effective security procedures in their products.

29. Governments and the private sector should regularly conduct vulnerability assessments and risk mitigation within all network systems. Risk assessments of supplier's products should be both technical and non-technical, taking into account the applicable legal environment and other aspects of supplier's ecosystem, as these factors may be relevant to government and private-sector efforts to maintain security.

30. Government policy should adopt policies that avoid "monocultures" across a country's network infrastructure and encourage a diverse and sustainable supply chain of trusted and secure manufacturers for network and system components. However, diversity requirements do not overcome the need for risk mitigation strategies for high-risk vendors.

31. Governments should encourage and support the adoption of best security practices for network operators and the implementation of security measures found in existing telecommunications standards (including secure network design and architecture, rules on

secure operation, and monitoring of and limitations on the outsourcing of functions).

Note: These criteria were developed by a group of private-sector experts from companies and research institutions in the United States, Europe, and Asia assembled by the Center for Strategic and International Studies.