MAY 2020

Criteria for Security and Trust in Telecommunications Networks and Services

CSIS Working Group on Trust and Security in 5G Networks

At the request of the Department of State, CSIS assembled a group of 25 experts from Asian, European, and U.S. 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 opportunities 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.

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

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 the 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 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 an 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 acquisition 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 an 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 and were assembled by the Center for Strategic and International Studies.

Project Director

James Andrew Lewis

Senior Vice President and Director, Technology Policy Program
Center for Strategic and International Studies, Washington, D.C.

This report is made possible by general support to CSIS. No direct sponsorship contributed to this report.

This report is produced by the Center for Strategic and International Studies (CSIS), a private, tax-exempt institution focusing on international public policy issues. Its research is nonpartisan and nonproprietary. CSIS does not take specific policy positions. Accordingly, all views, positions, and conclusions expressed in this publication should be understood to be solely those of the author(s).