Annex to the Joint Statement Supplement of the Digital Economy Working Group for the 58th U.S.-Japan Business Conference:

Recommended Principles to Establishing "Trust in ICT Suppliers"

Various factors are relevant to assessing whether companies that manufacture, distribute, sell, or supply (collectively "Suppliers") ought to be treated as trustworthy sources of supply for technologies that enable the development and operation of critical ICT networks. Suppliers are "Trustworthy" when:

1. Technical risks associated with the Suppliers' products or services are reasonably understood and properly managed:
    a. Technology is designed, developed, and deployed pursuant to a transparent, testable, open, consensus standards-based, and process-oriented framework for identifying, assessing, and managing risk through the anticipated lifecycle of the product or service, including:
        i. Protection of development and build environments against compromises to production systems;
        ii. Adoption of a "controls framework" aligned to global industry standards (e.g., ISO 27001), including implementation of granular, role-based access controls;
        iii. Scanning of code for known vulnerabilities;
        iv. Modeling of anticipated threats and risks; and
        v. Maintenance of security of software and firmware update mechanisms and pathways.
    b. Provenance, pedigree, and integrity of code, including open-source code, can be reasonably demonstrated to ensure securability of resulting products and compliance with intellectual property rights;
    c. Technology is capable of standards-based conformance testing of controls implemented to manage risk—and also of ensuring repeatability of build processes such that tested code can be validated against code in a finished offering deployed and used in an operating environment;
    d. Verifiable technical measures are implemented to ensure the application of access controls that effectively limit access to authorized users, authorized processes acting on behalf of authorized users, or authorized devices

e. Vulnerability handling, remediation, and disclosure policies consistent with international best practices are adopted, transparently communicated, regularly used, and capable of assessment to ensure compliance;
f. Information security and privacy practices for the protection of personal data and respecting individual rights are adopted, transparently communicated, and assessed to ensure compliance; and
g. Controls, mitigations, policies, and procedures adopted by the Supplier should be clearly communicated and flowed through to:
    i. Suppliers of components and source code included in its products;
    ii. Processors/sub-processors of confidential, proprietary, and/or personal data; and
    iii. Distributors, partners, and resellers who receive, install, integrate, sell, and/or maintain the Suppliers' technology in the market.
h. Stability of the supply of products and services is secured and business continuity planning is prepared.

2. Suppliers demonstrate adherence to generally recognized norms of corporate behavior, including:
    a. Public "codes of business conduct" outlining the Suppliers' core values, principles, and practices;
    b. Public trading of equity, or equivalent mechanisms, to ensure decision-making in accordance with commercial considerations with regard to procurement, investment, and contracting through transparency of ownership, partnerships, governance structures, and funding sources;
    c. Public demonstration of compliance with auditing and accounting standards generally adopted in the marketplace (e.g., Generally Accepted Accounting Principles or International Financial Reporting Standards) designed to ensure the absence of hidden, opaque, or otherwise non-commercially competitive sources of funding, financing, or subsidy;
    d. Internal governance mechanisms clearly articulated, enforced, and subject to external review demonstrating a commitment to protect:
        i. Security and privacy of users and customers against cyber-enabled attacks or other unwarranted intrusion;
        ii. Privacy and individual rights with transparency, fairness, and accountability;
        iii. Integrity of products, services, and data against theft, tampering, and unauthorized access;
        iv. Intellectual property against theft, infringements or misappropriation;
        v. Fair and open competition;
        vi. Environmental resources against damaging or unsustainable practices;
        vii. Human rights against forced or unfair labor practices; and
        viii. Good governance, public health and well-being.

3. Suppliers operate subject to both international commercial norms as well as national and international laws and standards, but make decisions on the basis of commercial

considerations and in response to market forces rather than undue direct governmental control or influence over internal governance and operations as demonstrated by:

a. Absence of arbitrary access to company data, facilities, resources, or operations and of mandates to cooperate with government directives – as demonstrated by transparency and reasonable access to due process mechanisms allowing for challenge of such demands to be heard by an independent judiciary or other neutral arbiter.
b. Absence of requirements to include government officials in corporate structures or decision-making processes that limit ability of Supplier to act as an independent entity operating under market-driven – as demonstrated by transparency and public disclosure of organizational/governance structure, ownership interests; and

4. Suppliers are headquartered, formed, and operate under the laws of a nation that:
    a. Govern networks and connectivity services by demonstrating respect for the rule of law, shown by clear legal or judicial limitations on the exercise of power by the government;
    b. Govern subject to the rule of law with adequate separation of powers protected by an independent judiciary or other neutral arbiter of due process and protected rights; and
    c. Uphold internationally agreed norms, standards, and treaties essential to global human development, such as the UN Sustainable Development Goals —including being good stewards of environmental resources, implementing fair labor practices, protecting intellectual property, protecting public health and well-being and respecting privacy and human rights—in the procurement and acquisition of ICT.