CHAMBER OF COMMERCE
OF THE
UNITED STATES OF AMERICA

VINCENT M. VOCI
EXECUTIVE DIRECTOR, POLICY AND OPERATIONS
CYBER, INTELLIGENCE, AND SUPPLY CHAIN
SECURITY DIVISION

ABEL TORRES
SENIOR DIRECTOR
CENTER FOR GLOBAL REGULATORY COOPERATION

July 11, 2021

Email: cyber-review@dcms.gov.uk

Cyber Resilience Team - 4/47
Department for Digital, Culture, Media, and Sport
United Kingdom
100 Parliament Street
London
SW1A 2BQ

Subject: Supply Chain Cybersecurity

Dear Cyber Resilience Team:

The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing the interests of more than three million businesses of all sizes and sectors, many of whom are major employers and provide significant investment in the United Kingdom. At home and abroad, the Chamber is an acknowledged leader in digital economy policy, including digital trade, cybersecurity, data privacy, artificial intelligence, and e-commerce issues.

The Chamber welcomes the opportunity to comment on the Department for Digital, Culture, Media, and Sport's call for views on cybersecurity in supply chains and managed service providers. The Chamber views supply chain security and resilience as fundamental to both the economic and national security of the U.S. and our allies. Recent cyberattacks, impacting both public and private entities, have drawn attention to increasingly diverse and complex supply chains, underscoring the need for coordinated action by government authorities and the private sector. Coordinated efforts are necessary to enhance security, drive international collaboration, and hold malicious cyber actors accountable when they violate domestic and international laws.

To help businesses identify and mitigate third-party risk, the Chamber offers four key steps that organizations should include within a broader third-party management framework:

- **Build a Framework for Third-Party Categorization**. Third-party categorization helps inform supply chain managers of which third parties require a deeper assessment of their business activities and the size and criticality of the relationship.

- **Develop Workflow to Address the Intersection of Risk and Criticality**. Based on an established third-party categorization framework, risk managers can utilize cybersecurity tools to group organizations into portfolios where they can consider cyber risk and impact versus criticality together.
- **Frequent Assessments of High-Impact Suppliers**. Based on the combination of criticality and risk, third-party risk managers should establish a cadence for reviewing critical information.
- **Ensure Appropriate Risk Transfer**. Comprehensive third-party risk management programs frequently include insurance-based risk transfer. A simple approach to risk transfer considers the intersection of supplier risk and criticality and imposes insurance requirements on those suppliers whose combination requires additional protection. Risk mitigation is also an option, either through requiring increased controls at the third party or implementing controls at the primary organization.

Businesses rely on a complex, globally distributed, and interconnected third-party ecosystem. This ecosystem comprises various entities with outsourcing, diverse distributed routes, and various technologies, laws, regulations, policies, and processes interacting at digital and business speeds. Because supply chains differ significantly across and within organizations, these third-party risk management recommendations should not be viewed as a one-size-fits-all solution; instead, they should be tailored to the individual organizational context and implemented as part of an overall enterprise risk management plan.

Global supply chains have introduced new risks to the public and private sectors. The U.S. Department of Homeland Security ICT Supply Chain Risk Management Task Force issued a report last fall on lessons learned from the pandemic. Its key findings:

1. The pandemic has underscored the need for an approach that was already underway over the last six years: diversifying supply chains to a broader array of locations and away from single-source/single region suppliers.
2. The pandemic also exposed how some manufacturing companies were unprepared because of their reliance on lean inventory models, which have traditionally allowed for greater efficiency and cost-effectiveness.
3. COVID-19 also underscored the difficulties that companies face in understanding their junior tier suppliers and where they are located.

It is imperative that supply chain partners, such as operators, equipment manufacturers, and vendors, collaborate and are prepared to combat and mitigate expanding threats with evolving best practices to ensure a more secure and resilient digital ecosystem. Public-private partnerships are essential to enhance cybersecurity and ensure systems are updated and configured to deal with current threats.

Global governments are orienting themselves to address these risks, including the availability and integrity of networks, products, and systems; the security and resilience of the supply chains that support them; and confidentiality and privacy of data that flows over and through is stored on them. Our members share the United Kingdom's desire to protect the public, businesses, and critical national infrastructure through effective management of supply chain cybersecurity.

We believe that the U.S. government, the United Kingdom, and our international allies can—and must—foster trust and improve security through continued engagement with the private sector on technical and nontechnical risk identification and mitigation efforts, as well as the promotion of continued development of trusted technologies, services, and products. Given the increasing complexity of modern supply chains and progressively sophisticated malicious cyber campaigns, multiple factors are relevant to assessing whether companies that manufacture, distribute, sell or supply take the appropriate measures to enhance the security of the digital supply chain.

The Chamber has developed the attached Principles for Trustworthy ICT Suppliers, which focus on ensuring that supply chain networks are more resilient and mitigate and manage cyber risk. They are also intended to promote a vibrant, diverse, and trustworthy supply chain.

If you have any questions or clarify our positions, please contact Vince Voci, executive director for cyber policy and operations (vvoci@uschamber.com) and Abel Torres, senior director for global regulatory cooperation (atorres@uschamber.com).

Sincerely,

Abel Torres
Senior Director
Center for Global Regulatory Cooperation
U.S. Chamber of Commerce

Vincent Voci
Executive Director
Cyber, Intelligence, and Supply Chain Security Division
U.S. Chamber of Commerce

Enclosure: Recommended Principles for Trustworthy ICT Suppliers

U.S. Chamber of Commerce
Recommended Principles for Trustworthy ICT Suppliers

1. Technical risks associated with the Suppliers' products or services are reasonably understood and properly managed:
    a. Technology is designed, developed, and deployed according 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 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. Maintaining the security of software and firmware and updating 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. Vulnerability handling, remediation, and disclosure policies consistent with international standards are adopted, transparently communicated, regularly used, and capable of assessment to ensure compliance;
    e. 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
    f. Controls, mitigations, policies, and procedures adopted by the Supplier should be communicated and flowed through to:
        i. Suppliers of components and source code included in its products;
        ii. Processors/sub-processors of confidential, proprietary, and personal data; and
        iii. Distributors, partners, and resellers who receive, install, integrate, sell, or maintain the market's suppliers' technology.

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 per commercial considerations concerning 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-commercial 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 government intrusions;
    ii. Privacy and individual rights with transparency, fairness, and accountability;
    iii. Integrity of products, services, and data against tampering;
    iv. Intellectual property against theft 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. Public health and well-being.

e. APPA (Authorized Public Purpose Access): Enable data distribution (especially in the healthcare sector) where negative effects of inappropriate data use have been mitigated through an appropriate governance model for specific components of the data to be available in support of a public purpose objective.

3. Suppliers operate subject to both international commercial norms and national laws but make decisions based on commercial considerations rather than undue direct government control or influence over internal governance and operations as demonstrated by:
    a. Absence of arbitrary access to company data, facilities, resources, or operations and mandates to cooperate with government directives – as demonstrated by transparency and reasonable access to due process mechanisms allowing for the challenge of such demands to be heard by an independent judiciary or another neutral arbiter.
    b. Absence of requirements to include governmental or party officials in corporate structures or decision-making processes – 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 subject to the rule of law with adequate separation of powers protected by an independent judiciary or another neutral arbiter of due process and protected rights; and
    b. Uphold internationally agreed norms, standards, and treaties essential to global human development—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.