ITI Promoting Innovation Worldwide

Ms. Evelyn Remaley
Associate Administrator
National Telecommunications and Information Administration
1401 Constitution Ave NW
Washington, DC 20230

ITI Comment re: NTIA RFC on Promoting Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers; Docket No. 200609-0154

Dear Ms. Remaley,

The Information Technology Industry Council (ITI) appreciates the opportunity to respond to NTIA's Request for Comment on Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers.

ITI represents the world's leading information and communications technology (ICT) companies. We promote innovation worldwide, serving as the ICT industry's premier advocate and thought leader in the United States and around the globe. ITI's membership comprises top innovation companies from all corners of the technology sector, including hardware, software, digital services, semiconductor, network equipment, and other internet and technology-enabled companies that rely on ICT to evolve their businesses.

Most of ITI's members service the global market via complex supply chains in which technology is developed, made, and assembled in multiple countries, and service customers across all levels of government and the full range of global industry sectors, such as financial services, healthcare, and energy. We thus acutely understand the importance of securing global ICT supply chains as not only a global business imperative for companies and customers alike, but as critical to our collective security. As a result, our industry has devoted significant resources, including expertise, initiative, and investment in cybersecurity and supply chain risk management efforts to create a more secure and resilient Internet ecosystem. ITI's Senior Vice President of Policy, John Miller, also serves as the IT Sector Co-Chair of the Information and Communications Technology Supply Chain Risk Management Task Force, which is undertaking work that is highly relevant to this RFC.

It is through this lens that ITI offers its comments on the Communications Supply Chain Risk Information Partnership (C-SCRIP) program NTIA has been directed to set up by the Secure and Trusted Communications Act of 2019.

In our comments, we offer our perspective on: (1) the ways in which NTIA should interpret key terms, including supply chain security risk, trusted supplier or provider, and foreign adversary; (2) how to best facilitate information-sharing, including recommending a mix of in-person briefings and public updates; and (3) ways in which NTIA can best handle the issues associated with granting security clearances, including ensuring that information is not overclassified at the start and establishing tear lines that allow for greater information-sharing.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Key Terms

The way in which NTIA chooses to define or interpret key terms like "supply chain security risk," "foreign adversary," and "trusted supplier and provider" is incredibly important, particularly because it could set a precedent for the way these terms are defined and interpreted moving forward. We appreciate the opportunity to provide our perspective on the way that NTIA has indicated it will define these terms, and also provide responses to the specific questions posed by NTIA that are relevant to each term.

1) Supply chain security risk:

We appreciate NTIA's efforts to align itself with definitions put forth in the Federal Supply Chain Security Act of 2018. We also appreciate that NTIA will consider terms as defined by the ICT Supply Chain Risk Management (ICT SCRM) Task Force, which is undertaking work that will be helpful to executing this information-sharing program in a variety of ways.

a) *What sorts of risks and vulnerabilities should be covered by the language "specific risk and vulnerability information related to equipment and software"?*

As a threshold matter, what is most important is that any threats identified by NTIA be based on factual evidence of concrete risks – that is how we interpret the meaning of the term "specific." We recommend that NTIA look to the current work being undertaken by the ICT SCRM Task Force Threat Evaluation Working Group, whose goal is to establish a set of processes and criteria for evaluation ICT suppliers, products, and services. Last year, the group focused on establishing a catalogue of supplier-related threats, identifying nearly 200 different categories of such threats and it is currently working to establish an additional catalogue focused on threats related to products and services. We anticipate that it will identify many more product and services threats this year. This work will be particularly applicable to outlining specific risk and vulnerability information related to equipment and software. That said, the threat categories outlined that are relevant to supplier-related risk are also relevant to equipment and software and provide a good basis for NTIA to consider the sorts of risk and vulnerability information to include in any information-sharing program.

b) *What information, if any, is unique to "supply chain risk information"? In other words, to avoid the re-creation of existing threat and vulnerability information sharing programs, what types of specific, enhanced, or aggregated threat and vulnerability information would be helpful to the private sector to identify, avoid, or mitigate ICT supply chain risks? What information do suppliers and providers need to make informed, risk-based security and transactional decisions?*

There are various categories of information specific to supply chain risk that can help suppliers and providers make informed, risk-based security and transactional decisions and is not embraced by other information-sharing programs, e.g. existing information sharing programs that primarily deal with sharing cybersecurity threat indicators but do not share information on supplier threats.

ICT SCRM Task Force Working Group One has made excellent progress exploring the types of information that would be most valuable in mitigating supply chain risk, including whether that information exists in a standardized or easily accessible form or from sources that can be easily

identified, accessed and leveraged for risk management purposes, and what barriers might exist that are impeding the collection and or dissemination of such information. While Working Group One determined that many types of risk information are indeed available, the sources were not always easily known and did not typically exist in a standardized format (unlike cyber threat indicators in the cybersecurity threat information sharing context). Additionally, due to the wide array of supply chain threats, such information was not easily centralized nor accessible. Working Group One significantly determined that the highest value supply chain threat information relates to suspected, known, or proven bad actors in the supplier context, but that legal and policy issues often prevent the sharing of such information. The Working Group concluded that further legal analysis and guidance are thus prerequisite to fully developing the envisioned bi-directional supply chain information sharing framework. This foundational work has been carried forward into year two of the Task Force and should be factored into NTIA's analysis.

2) Foreign adversary:

While we understand that NTIA intends to rely upon the definition of "foreign adversary" as outlined in Executive Order 13873, we would refer NTIA back to our comments in response to the ICTS Supply Chain NPRM, in which we outlined our concerns with the way foreign adversary is defined.[1] As a general matter, we recommended against designating entire countries as foreign adversaries, and instead recommended that the government should revise the definition of foreign adversary to foreign adversary *person,* which means any foreign non-government person[2] determined by the Secretary to (1) be owned by, controlled by, or subject to the direction or influence of a foreign adversary government entity, and (2) have engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons for the purposes of Executive Order 13783. In those comments, we also note that one of the significant shortcomings of that Rulemaking is it fails to establish any process or lay out any criteria by which the Secretary may designate foreign adversaries.

3) Trusted supplier or provider:

While we appreciate that NTIA is attempting to maintain consistency with existing designations, we would caution NTIA, when defining a "trusted supplier or provider," to avoid depending too heavily on whether a company formally attests to compliance with subsection(a)(1)(B) of the *John S. McCain National Defense Authorization Act for Fiscal Year 2019* or on E.O. 13873, especially given the very broad and vague criteria laid out in both policies. Because the designation of one or more "foreign adversaries" is a necessary prerequisite for the Secretary to exercise his authority to prohibit, block, or unwind any ICTS transaction pursuant to the EO, the designation of one or more foreign adversaries is a key threshold criterion that must be satisfied prior to determining whether a nexus to a foreign adversary exists. Right now, there is no such process in place by which foreign adversaries will be designated, nor are any foreign adversaries identified in the NPRM. Thus, relying on E.O. 13873 is somewhat unhelpful to determine a "trusted supplier or provider." As we referenced in our comments to both the ICTS Supply Chain NPRM as well as to the NTIA RFC on the *National Strategy to Secure 5G*, it may be helpful to consider factors that make a supplier more or

[1] https://www.itic.org/dotAsset/d6447508-0425-4848-b968-4f91490b8494.pdf

[2] "Person" is defined in §7.2 of the proposed rules as "an individual or entity," and "entity" is defined as "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization."

less trustworthy (or a transaction more or less risky). Please see below for factors to consider when evaluating or determining trustworthiness.

a) *Are there other factors aligned with the Act that should be considered in determining "trusted" providers and suppliers eligible for the program?*

In response to this question, we refer NTIA to the comments we submitted to the RFC on the *National Strategy to Secure 5G*, where we address the idea of "trustworthiness."[3] To reiterate here, "trustworthiness" has many dimensions and should therefore be viewed in a way that moves beyond solely considering country-of-origin. While country-of-of-origin is one risk factor to be considered, it is not the sole and dispositive factor. Indeed, after a year of study the ICT SCRM Task Force working group on Threat Evaluation catalogued 188 supplier related threats.[4] While one of these factors was appropriately the country of origin of a supplier, it would be a mistake to not take a holistic view of the supply chain threat and risk landscape when evaluating the trustworthiness of a particular provider. In fact, the practices of a vendor -- how securely a vendor develops its products and services within a wider culture of security and recognized development best practices – should be the priority and focus, as this is a more reliable indicator of the security of products/services than a mere examination of the product/service itself.

Other factors to consider when evaluating the trustworthiness of a supplier or provider include the geopolitical implications of manufacturing locations, a supplier's adherence to international standards, a supplier's cybersecurity, enterprise risk management and secure development practices, and other supply chain threat vectors identified by the Task Force.[5] Whether a company signed National Security Agreement with the United States, or whether a company is incorporated under a Mutual Defense Treaty as an allied nation are also indicators that should be heavily weighted in favor of trustworthiness. We would strongly encourage NTIA to review and incorporate elements of the Threat Scenarios Report prepared by the ICT SCRM Threat Evaluation Working Group referenced above. We believe this assessment is a useful tool for policymakers and industry alike to understand the full range of threats that may impact a supplier and that can help to inform trustworthiness evaluations.

Information Sharing Policies and Procedures

In general, we agree that this program should focus on sharing information with small and rural providers and suppliers, who may have more difficulty accessing information than larger, more sophisticated and better resourced providers and suppliers. However, to the extent this program can be structured so as to not be duplicative of existing information sharing programs that larger suppliers already participate in, such as VEPS, it could be useful for larger providers and suppliers, we encourage NTIA to consider expanding the scope.

We reiterate our encouragement to NTIA to leverage the work undertaken by Working Group 1 of the ICT SCRM Task Force, which is focused on bidirectional information-sharing. While we recognize that the remit of the Act is to facilitate the sharing of information from the Federal government to

[3] https://www.itic.org/policy/ITICommentstoNTIARFC5GStrategy.pdf
[4] https://www.cisa.gov/sites/default/files/publications/ict-scrm-task-force-threat-scenarios-report_0.pdf
[5] https://www.cisa.gov/publication/ict-scrm-task-force-interim-report

suppliers and providers, there are useful findings stemming from those discussions that could be applicable to this information-sharing program, including an exploration of the types of information that would be most useful to share and receive. More specifically, Working Group One concluded that facilitating the sharing of information related to suspected, known or proven bad actors would be most valuable.[6] Please see our response to Question b on page 2 for additional information.

a) *What means of sharing information best balances the objectives of the Act and the need to safeguard sensitive information? More specifically, what are the best ways for the Federal government to provide "regular briefings" to providers and suppliers? Would periodic public updates or notifications be useful or sufficient?*

In this context, it is our view that a mix of periodic in-person briefings and public updates or notifications is necessary. It may be helpful for NTIA to consider creating an unclassified, open source product line aimed at small providers, potentially similar to the CISA product line on Cyber Essentials.[7] The CISA product line is intended to be a guide for small and medium-sized enterprises considering how to implement organizational cybersecurity practices. We believe a similar product line would be a very useful way to disseminate potentially complex information to small providers in an understandable and easily digestible format, i.e., a program that focused on providing the absolutely minimal essential supply chain threat related information that would be useful for small and rural providers to know.

Further, we recommend that in its effort to provide regular briefings, NTIA (and the USG more broadly) seek to declassify as much information as possible and/or figure out how to most appropriately calibrate the classification tear lines in order to prioritize getting useful information out to as broad an audience as possible. Overclassification remains an issue and precludes many companies, especially small and rural providers who may not have cleared personnel, from accessing information that could help them make risk-based, transactional decisions.

b) *Should eligible providers and suppliers have an opportunity to request risk and vulnerability information about specific equipment, software, and services? Would an information sharing system that incorporates both "push" and "pull" capabilities be useful, if possible?*

This suggestion seems like it would be practically useful, provided such information could be provided in a way that is consistent with companies' proprietary and competitive business interests.

c) *Are there legal barriers that could impede the ability of trusted providers and suppliers to receive or act on security risk information from the Federal government?*

There may be legal barriers that could impede the ability of trusted providers and suppliers to receive or act on security risk information from the Federal government. In particular, NTIA should evaluate whether any of the legal barriers that emerged and were addressed during the previous debates over cybersecurity threat information sharing circa 2011-2015 may be applicable and need to be revisited in the context of a new, supply chain threat information sharing program. In

[6] https://www.cisa.gov/publication/ict-scrm-task-force-interim-report
[7] https://www.cisa.gov/cyber-essentials

particular, some of the perceived barriers addressed in the *Cybersecurity Information Sharing Act of 2015*[8] included issues more relevant to sharing by companies to the government, including privacy, liability, FOIA, antitrust and regulatory use issues, depending on the sources of government-provided information and the structure of the NTIA program some of these issues may need to be revisited. In particular, depending on the sources, type and scope of information shared NTIA should make sure to address any perceived privacy issues relating to that data, and adopt safeguards such as minimization procedures to address any implicated personal data. Additionally, one of the important findings of the ICT SCRM Task Force Information Sharing Working Group was that there are legal considerations that must be addressed with regard to sharing and/or receiving "potentially derogatory, supplier-specific" information, although it should be noted that finding was more specific to the context of information provided by one private sector entity to another.[9]

d) How can publicly available security risk information be conveyed more expeditiously to more small and rural providers and suppliers?

See our recommendation above with regard to putting out periodic Cyber Essentials updates, and the importance of declassifying as much information as possible so it can be readily distributed to a wider audience of suppliers and providers. Establishing a program to facilitate the distribution of unclassified threat information would make it easier to explore distribution methods such as setting up an email notification system where enrolled providers can receive up-to-date information on supply chain-related threats.

Another option worth exploring is to set up a secure web portal where approved providers and suppliers could log in using credentials to receive unclassified FOUO threat information. DHS's Homeland Security Information Sharing Network (HSIN)[10] program, a system for trusted sharing of Sensitive But Unclassified information between federal, state, local, territorial, tribal, international and private sector partners, could be another model for NTIA to consider. Finally, great strides have been made in developing automated information sharing programs, such as the program established by the *Cybersecurity and Information Sharing Act of 2015* that relies on STIX/TAXII protocols to distribute cyber threat indicators in an automated fashion. NTIA should explore whether the types of information shared via the contemplated program could be shared in an automated format, and whether a similar automated program is viable or potentially more efficient than sharing information via email or a portal.

e) What barriers (e.g., awareness, financial, legal) do small and rural providers and suppliers face in accessing security risk information from non-government sources? What could or should the Federal government do to eliminate or mitigate those barriers?

As discussed above, there are a variety of potential legal impediments that may prevent small and rural providers from accessing threat information relating to suppliers from other private sector entities (as indicated in our discussion of the Task Force WG 1 efforts above).

[8] https://www.congress.gov/bill/114th-congress/senate-bill/754
[9] https://www.cisa.gov/publication/ict-scrm-task-force-interim-report
[10] https://www.dhs.gov/homeland-security-information-network-hsin

Security Clearances

As a general matter, we believe that there is a need for holistic, government-wide security clearance reform.

The current system for processing security clearances for work with various government agencies is opaque, unpredictable and burdensome in that it is often overly dependent on nontransparent decisions made by Contracting Officers and subject to unreasonable delays of months and in some cases years. While additional bifurcation of the process would only cause further delay, inefficiency, and potentially create greater vulnerabilities, we appreciate both that NTIA is likely not in a position to solve the longstanding government-wide issues regarding clearances and that NTIA is tasked with presenting a plan for declassifying information and expediting security clearances to facilitate information-sharing to trusted providers and suppliers.

With that in mind, we recommend that NTIA (and the U.S, government more broadly) seek to avoid overclassifying information from the start. The declassification process will be made much easier if information is not overclassified from the outset. Oftentimes, due to the risk-averse nature of the government, national security information appears to be classified at a level higher than necessary. This can cause confusion about who the information can be shared with and stifles the ability to share otherwise actionable information within and outside of the U.S. government.

Of course, much information is appropriately classified by the government. However, a greater effort could be made to establish tear lines that allow the key higher-level elements of supply chain threat information to be shared with small and rural providers while protecting intelligence sources and methods.

Conclusion

Once again, ITI is pleased to submit comments in response to NTIA's RFC on the C-SCRIP. Information-sharing is an incredibly important tool in mitigating supply chain risk, and we appreciate NTIA's efforts to establish a program to help facilitate the exchange of useful, actionable information with smaller providers. We hope that our recommendations will be helpful as NTIA seeks to implement the C-SCRIP program and remain a willing partner and resource moving forward.

Sincerely,

John S. Miller
Senior Vice President of Policy
and Senior Counsel

Courtney Lang
Director of Policy