Before the Department of Commerce
National Telecommunications and Information Administration
Washington, D.C.

PROMOTING THE SHARING OF SUPPLY	)	
CHAIN SECURITY RISK INFORMATION	)	**NTIA Docket No. 200609-0154**
BETWEEN GOVERNMENT AND	)	**RIN 0660-XC046**
COMMUNICATIONS PROVIDERS AND	)	
SUPPLIERS	)	

The Communications Sector Coordinating Council ("CSCC")[1] commends NTIA for seeking to establish, in cooperation with other designated federal agencies, a program to share supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services.[2]

We further commend NTIA for choosing to focus on trusted providers and suppliers that are small businesses and those primarily serving rural areas, consistent with the call for engaging these entities within Section 8 of the Secure and Trusted Communications Network Act of 2019.

Our comments provide answers to several individual questions asked by NTIA pertaining to strategies for creating this information-sharing program. While a variety of business' views are included, there is a principal focus on those of the Small and Medium Business (SMB) community since those entities are the principal focus of the program.

1. *Key Terms*

Q: NTIA seeks comment on clarifying the term ''trusted providers and suppliers.'' The Act requires information sharing only with ''trusted'' providers and suppliers—entities ''not owned by, controlled by, or subject to the influence of a foreign adversary.''

A: While industry does not provide or promote a specific definition, the sector urges that the U.S. government offer clarity about any countries or entities that constitute foreign adversaries for predictability and consistency.

[1] The members of the CSCC broadly represent the sector and include cable, commercial and public broadcasters, information service providers, satellite, undersea cable, utility telecom providers, service integrators, equipment vendors, and wireless and wireline owners and operators and their respective trade associations.

[2] *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, NTIA Docket No. 200609-0154, 85 Fed. Reg. 35919 (June 12, 2020); *Notice, Extension of Comment Period*, NTIA Docket No. 200609-0154, 85 Fed. Reg. 40625 (July 7, 2020).

Q: What sorts of risks and vulnerabilities should be covered by the language ''specific risk and vulnerability information related to equipment and software''?

A: The risks and vulnerabilities shared should be actionable and verifiable. They could relate to software vulnerabilities, suspected malware, hardware concerns, indications of problems in the security of updates and patches, or other security concerns. Additionally, industry could benefit from information about observed efforts to compromise systems of suppliers or vendors, as well as information about overseas manufacturing issues or foreign adversary government directives would also be helpful.

Q: Are there other factors aligned with the Act that should be considered in determining ''trusted'' providers and suppliers eligible for the program?

A: Broadband internet access providers that are subject to the Communications Act, as regulated by the FCC, should be deemed trusted providers. Also, a company's participation in an information sharing analysis center such as the Communications ISAC.

2. *Information Sharing Policies and Procedures*

Q: 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?

A: The approach to be adopted should be flexible and involve a combination of activities. In particular, the government should offer a variety of approaches to help small and rural providers. For certain types of information, the government should consider whether the underlying classification system should be reviewed. Declassified information could be shared with points of contact across industry. Other sharing may require briefings by government officials to company personnel, in which case the government needs to carefully consider how it can provide actionable and verifiable information without the need to bring a company employee to a SCIF or have a cleared representative.

Additionally, mirroring security concern "alerts" to alerts currently used to make communications providers and other interested parties aware of security vulnerabilities, such as those issued by the Cybersecurity and Infrastructure Security Agency ("CISA") through US-Cert.gov, would be a useful step for notifying providers and suppliers using a known, trusted forum by which to receive notices of security concerns.

To provide more in-depth reports of information security concerns, NTIA in coordination with other federal agencies engaged in securing the nation's communications infrastructure against cyber threats should establish a single source for "briefings" that focuses solely on communications providers and suppliers, which will allow the source to become recognized by providers and suppliers as a trusted source for information about federal security concerns.

By limiting the information relayed by NTIA or any other appropriate government agency to non-classified, public information, any concerns related to sharing such information with the public should be avoided. However, in order to track the entities receiving the information, NTIA or the entity disseminating the information could require any entity wishing to receive emails pertaining to supply chain risks to first register their name and email address with the entity providing the emails. NTIA and other federal agencies could also further awareness of security risks by working with trade associations to identify and share sector-specific security risk information and concerns.

Q: 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?

A: The option to request information about specific equipment, software, and services would be helpful because companies make procurement decisions at varied times and may not have a robust internal capability to manage supply chain risk. However, it would be important that such an option does not create the expectation that companies will seek government pre-approval for procurements. Furthermore, when an entity requests information about a supplier for security reasons, US government agencies should refrain from using anti-trust concerns as a reason not to share information in a timely way with the requesting entity. Moreover, the. government would have to develop a way to keep requests confidential, as equipment and supply chain decisions are usually confidential and proprietary.

An information sharing system that incorporates government push capabilities would be useful, alongside or independent from pull capabilities. If the information sharing system incorporates push capabilities, then updates will occasionally be necessary; participating trusted providers and suppliers may consider including these updates as part of their Business Continuity Plan (BCP).

Q: 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?

A: The DHS ICT Supply Chain Task Force WG 1 – Information Sharing ("WG1") is working on these issues. The Federal Acquisition Security Council is also tasked with developing recommendations on information sharing. WG1 found that, in addition to providers' receipt of security risk information from the federal government, having the ability to share equipment or product security concerns with other providers or the federal government early, and prior to the federal government publicly identifying a security threat, can minimize disruptions to providers' operations. However, providers risk legal action by sharing these concerns. The government can encourage this important information sharing by decreasing the risk of litigation using the following methods: (1) educating communications providers and suppliers about existing security threats; (2) coordinating two-way information sharing between the federal government and the CSCC for the dissemination of supply chain security risk information; (3) establishing a new organization within the Department of Homeland Security or Department of Commerce that would act as a clearinghouse for supply chain risk and threat information; and (4) working with Congress to enact a new law that would protect providers from legal action when sharing supply chain risk and threat information. Although each of these methods would require the specific details to be addressed, and some, such as enacting a new law, could take a year or more to become reality, the instant proceeding and the Act's requirement that NTIA work with other federal agencies to establish a method of sharing supply chain security risk information with trusted providers of advanced communications service and suppliers of communications equipment or services provides the opportunity and necessity to begin implementing these methods

Given the voluntary nature of NTIA's proposed information-sharing program, NTIA should also make clear that a company's receipt of information from the government creates no duty, implied or otherwise, to act; that any failure to act by a recipient cannot constitute negligence; and that information provided is not of the type that would give rise to a mandatory disclosure as a risk factor.

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

A: Small and rural providers should be encouraged to join relevant associations and existing information sharing venues such as information sharing analysis centers (ISACs) and information sharing analysis organizations (ISAOs) (including CSCC and the Communications ISAC), perhaps in working groups that focus on their needs, such as the CSCC Small and Mid-Size Business Committee . Many of these venues, including the CSCC, are free to join. Additionally, NTIA and other federal agencies engaged in sharing supply chain security risk information could work with trade associations whose members include Trusted Providers to help disseminate information to a large number of Trusted Providers.

Q: 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?

A: The products and programs that various commercial sources offer may not be economical or necessary for each small provider to invest in since they vary in scope and quality. Large telecoms and suppliers are able to establish robust risk management programs that include third party assessments and consultants. Since the SMB community is less equipped to make such an investment, it is especially important for the government and relevant venues to disseminate actionable information.

3. *Information and Declassification and Security Clearances*

Q: How specific must security risk information be to enable providers and suppliers to make procurement decisions that adequately protect their networks, customers, and users? If, for example, the Federal government issues a security warning about a particular company, how much information do trusted providers or suppliers require about the reason for that warning in order to take appropriate action?

A: Alerting providers and suppliers to the name of the company and the make/model of the products/services with whom the federal government has information security concerns would be most helpful to small and mid-size providers and would likely allow the information to be disseminated more quickly than a more detailed report listing reasons for the concerns given the limitations on information sharing due to the risk of legal action. However, to ensure providers receive any essential information as early as possible, if releasing the make/model of the products/services would delay government's ability to share the name of the company with providers – absent a security clearance – CSCC recommends the government initially share the company name and follow up with additional information about the make/model of the products/services as soon as it is able to share such information publicly.

Whenever possible, the information should be specific enough to enable providers to verify the risk. In particular, information about when a risk was discovered could be important for determining whether the risk is timely and actionable. Generic information about countries of concern may not be actionable or may not come at the right time relative to a decision.

Q: Is it more helpful for small and rural providers to receive unclassified information through typical civilian channels (for example, by email) or to receive more detailed classified information that would require a staff member to obtain a security clearance and could require travel to receive the classified information in person at a secure location?

A: It may be preferable for the government to withhold as little actionable information as possible when sharing information through civilian channels, since classified access is often not more useful than what is publicly available and such a solution would reduce the number of barriers in the SMB community.

Employees at many small and mid-size providers typically wear multiple hats and do not have the luxury of focusing exclusively on cybersecurity issues, including being on the "lookout" for potential security concerns. Accordingly, small and mid-size providers would benefit from information related to security concerns emanating from a single federal government source. Furthermore, identifying a resource within the federal government for small and mid-size providers to consult regarding supply chain security threats, whether identified by the federal government through an alert or other notification method, or perceived by the provider, and that could offer suggested alternatives for any equipment or software deemed a threat by the federal government, would help achieve the goal established by the Act of "ensuring that [small, rural providers] have access to the information they need to keep their networks and Americans secure."[3] Ultimately, small and mid-size providers would benefit the most from the federal government making them aware of the names of the companies and make/model of the equipment the government has identified as posing a security threat, rather than the providers needing to obtain a security clearance in order to learn the reasons behind such a determination.

Q: What would be the best way of identifying appropriate staff points of contact at small and rural providers to ensure that they receive security risk information?

[3] *Id*. at 35921.

A: If NTIA is looking for ways to directly contact providers, it should work with the FBI, which shares security risk information through partnerships such as InfraGard, and the FCC, which may have points of contact, such as from the Systems Security and Integrity Plans that are submitted to the FCC to facilitate compliance with CALEA. In general, though, there is no one-size-fits-all approach to contacting small providers, so establishing a person of contact may need to be handled on a one-on-one basis.

Q: Have small and rural providers and suppliers encountered problems in attempting to obtain security clearances for staff? If so, what has been the nature of those difficulties?

A: Small and rural providers do not have the resources to request a security clearance for staff members and staff members at small providers often take on myriad responsibilities and would therefore be unable to devote the time and attention needed to participate in government security briefings necessary to remain aware of more high level security concerns. Additionally, even large providers who have the time and resources to devote to an employee's security clearance, have encountered slow review of security clearance applications. This slow review is an area that merits immediate and aggressive attention, as has been called for over many years by the Communications Security, Reliability, and Interoperability Council's (CSRIC), the National Security Telecommunications Advisory Committee (NSTAC), and other groups.

Q: How should NTIA best raise awareness of this program among small business and rural providers?

A: Through organizations such as the CSCC, Communications ISAC, and various associations, NTIA will be able to raise awareness of this program to a wide and inclusive range of SMB companies. NTCA – The Rural Broadband Association ("NTCA"), for instance, a member of the CSCC, represents approximately 850 independent, community-based telecommunications providers in the most rural portions of the United States, all of whom provide broadband internet service to their communities. Through NTCA's participation in the CSCC, NTCA is able to relay information from government entities such as CISA and NIST to its members and vice versa. Other trade associations (e.g., USTelecom, NCTA, CTIA, TIA) also have small and medium business members and can be effective platforms to raise awareness among their members.

In conclusion, an awareness of supply chain security risk information is essential to all communications providers regardless of size and the earlier providers are made aware of, or can share knowledge or suspicions they have regarding security concerns, the less damage will be done to providers, suppliers and members of the public who rely on the providers' networks for everything from work to school to healthcare to communicating with friends and family. Accordingly, the CSCC welcomes the instant Request for Comments and the opportunity to engage further with NTIA and other federal agencies to develop and expand information sharing in a manner that reaches all trusted providers.

Sincerely,
COMMUNICATIONS SECTOR COORDINATING COUNCIL

Robert L. Mayer

Robert Mayer
Chairman
Communications Sector Coordinating Council

Kathryn Condello

Kathryn Condello
Vice Chairman
Communications Sector Coordinating Council

July 28, 2020