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

In the Matter of	)	
	)	
Promoting the Sharing of Supply Chain	)	Docket No. 200609-0154
Security Risk Information between	)	RIN: 0660-XC046
Government and Communications	)	
Providers and Suppliers	)	

COMMENTS OF CTIA

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

Melanie K. Tiano
Director, Cybersecurity and Privacy

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

July 28, 2020

Table of Contents

I. INTRODUCTION AND SUMMARY

CTIA[1] is pleased to comment on the National Telecommunication and Information Administration's ("NTIA") Request for Comments ("RFC") on Promoting the Sharing of Supply Chain Security Risk Information, under Section 8 of the Secure and Trusted Communications Network Act of 2019 (the "Act"),[2] which directed NTIA to establish "a program to share information regarding supply chain security risks with trusted providers of advanced communications service and trusted suppliers of communications equipment or services."[3]

Despite the pendency of this RFC, NTIA announced the Communications Supply Chain Risk Information Partnership ("C–SCRIP") in a Notice published on July 8, 2020 ("July 8 Notice").[4] It describes "a partnership to share supply chain security risk information with trusted communications providers and suppliers" that NTIA expects to roll out in four phases.[5]

- Phase One will establish the program and develop the required report to Congress on NTIA's plan to work with interagency partners on: (1) declassifying material and (2) expediting and expanding the provision of security clearances.
- Phase Two will operationalize the program, "informed by public comments."[6]

---

[1] CTIA® (www.ctia.org) represents the U.S. wireless communications industry and the companies throughout the mobile ecosystem that enable Americans to lead a 21st century connected life. The association's members include wireless carriers, device manufacturers, and suppliers, as well as apps and content companies. CTIA vigorously advocates at all levels of government for policies that foster continued wireless innovation and investment. The association also coordinates the industry's voluntary best practices, hosts educational events that promote the wireless industry, and co-produces the industry's leading wireless tradeshow. CTIA was founded in 1984 and is based in Washington, D.C.

[2] Secure and Trusted Communications Networks Act of 2019, H.R. 4998, Pub. L. 116-124 (Mar. 12, 2020) ("Secure and Trusted Communications Networks Act").

[3] National Telecommunications and Information Administration, Promoting the Sharing of Supply Chain Security Risk Information, 84 Fed. Reg. 35919 (June 12, 2020), https://www.govinfo.gov/content/pkg/FR-2020-06-12/pdf/2020-12780.pdf ("*RFC*").

[4] National Telecommunications and Information Administration, Establishment of the Communications Supply Chain Risk Information Partnership, 85 Fed. Reg. 41006 (July 8, 2020), https://www.govinfo.gov/content/pkg/FR-2020-07-08/pdf/2020-14725.pdf ("*July 8 Notice*").

[5] *Id.*

[6] *Id.*

- Phase Three will refine methods for generating and sharing information within the C–SCRIP, formalize briefings and alerts, and establish mechanisms for ongoing coordination.
- Phase Four will evaluate the initiation period and make recommendations for adjustments.

Congress intended that NTIA have the benefit of public comment as it establishes the new information sharing regime and these comments should drive NTIA action.[7] We encourage NTIA to consider these and all comments before it proceeds with the C–SCRIP, including Phase One.

CTIA urges NTIA to (1) promote the sharing of actionable, verified, and timely information with a broad array of communications sector stakeholders; (2) lead efforts to push long-overdue changes to the way the government extends security clearances and declassifies information; (3) look for ways to broaden participation in existing information sharing efforts rather than create a siloed approach that could fragment information sharing; and (4) help the Executive Branch harmonize overlapping supply chain efforts.

II. IT IS IMPERATIVE THAT THE FEDERAL GOVERNMENT SHARE ACTIONABLE INFORMATION WITH THE PRIVATE SECTOR

A. There is consensus that the Federal government must increase information sharing with the private sector.

Information about cybersecurity and national security is vital to the "collective defense" and public private partnerships that have been a bedrock of federal policy. Unfortunately, difficulties obtaining private security clearances and declassifying information have prevented the government from disseminating actionable information to the private sector, leaving private actors to fend for themselves against foreign, state-sponsored threats. As the concerns have

[7] Secure and Trusted Communications Networks Act §8(a)(1) ("Not later than 120 days after the date of the enactment of this Act, including an opportunity for notice and comment, the Assistant Secretary… shall establish a program." (emphasis added)).

expanded to security threats posed by nation-state affiliated telecommunications companies, the government needs to resolve longstanding issues. It is encouraging that NTIA's July 8 Notice states that "NTIA will coordinate closely with its federal partners to take advantage of the existing processes and procedures in place for the processing of security clearances and the declassification of threat intelligence." CTIA urges NTIA to be creative in pushing other agencies to issue clearances and to disseminate more information. Congress in Section 8(a)(2)(C) of the Act directed the submission to Congress of a plan to increase declassification of information about supply chain security risks and expedite and expand security clearances. That report is due September 8 and CTIA looks forward to opportunities to assist NTIA with those issues.

Public-private forums have concluded for years that the Federal government must increase the amount of timely, verified, and actionable information shared with the private sector in order to stave off threats from foreign actors. The National Security Telecommunications Advisory Committee ("NSTAC") has called for "a national resource for threat collection and analysis that produces actionable intelligence and measures that can be utilized across the whole-of-nation (not just whole-of-government . . .) at the unclassified level."[8] The Federal Communications Commission's ("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") examined information sharing years ago and observed that "not having knowledge of and access to classified information may have an effect on business activities. Classified information should be downgraded and distributed where possible."[9]

[8] NSTAC, NSTAC Report to the President on Advancing Resiliency and Fostering Innovation in the Information and Communications Technology Ecosystem, at 27 (Sept. 3, 2019), https://www.cisa.gov/sites/default/files/publications/nstac_letter_to_the_president_on_advancing_resiliency_and_fostering_innovation_in_the_ict_ecosystem_0.pdf

[9] CSRIC V, Working Group 5: Cyber Security Information Sharing, Final Report, at 4 (June 2016), https://transition.fcc.gov/bureaus/pshs/advisory/csric5/WG5_Info_Sharing_Report_062016.pdf ("*CSRIC V Working Group 5 June 2016 Report*").

CSRIC offered numerous recommendations to address logistical and legal barriers to better information sharing.

More recently, the Cyberspace Solarium Commission ("Solarium Commission") observed that "the U.S. government must address more general limitations in its ability to provide intelligence support to all private sector stakeholders and associated organizations, such as information sharing and analysis centers ("ISACs")."[10] The Solarium Commission recommended that Congress direct the Executive branch to conduct a six month comprehensive review of any such limitations on the ability of the intelligence community to provide intelligence to the private sector.[11] While this is a helpful step, this is not aggressive enough.

Congress too has emphasized the importance of information sharing. In addition to the Act that is the subject of this proceeding, the 2015 Cybersecurity and Information Sharing Act envisioned bi-directional information sharing,[12] and the 2018 SECURE Technology Act called for the Federal Acquisition Supply Council[13] to identify or develop "criteria for sharing information with . . . non-Federal entities with respect to supply chain risk."[14] As supply chain and geopolitical concerns evolve, the government has a duty to share information with domestic companies and allied countries before investments are made.

B. Despite efforts, there remains a need for actionable, verified, and timely

[10] Cyberspace Solarium Commission, Final Report, at 99 (Mar. 2020) https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view ("Solarium Commission Recommendations").
[11] *Id.*
[12] Cybersecurity Information Sharing Act of 2015, S.754, (passed Senate by a 74-21 vote Oct. 27, 2015); incorporated into the Consolidated Appropriations Act, 2016, H.R. 2029, Pub. L. 114-113 (Dec. 18, 2015).
[13] The Federal Acquisition Security Council is an interagency council, chaired by the Office of Management and Budget ("OMB"), created by Congress in the Federal Acquisition Supply Chain Security Act of 2018, 41 U.S.C. §§ 1321-28. The Council's functions including identifying or developing criteria for sharing information with federal agencies, other federal entities, and nonfederal entities about supply chain risk and making recommendations to senior officials about the exclusion of sources or covered articles from procurement actions.
[14] Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act (SECURE Technologies Act), H.R. 7327, Pub. L. 115-390 (Dec. 21, 2018).

information sharing by the government.

CTIA is encouraged by the July 8 Notice stating that "NTIA will aim to ensure that the risk information identified for sharing under the program is relevant and accessible," but CTIA urges NTIA to prioritize verified and actionable information. Trustworthy information about security and supply chain is critical, yet, despite the private sector being inundated with reports purporting to identify security risks, many of these reports are unverified or not actionable.[15] Vendors gather and sell threat intelligence, however, global supply chain information is hard to qualify without government assistance.

The Department of Homeland Security ("DHS") issues alerts, bulletins, and Binding Operational Directives[16]—which provide helpful information for industry—but it also shares news reports and academic articles that may not be verified, actionable, or timely. DHS and other federal agencies do not offer a single or centralized source of reliable cybersecurity threat information, much less a solid framework for assessing global supply chain risks from nation states. When it comes to communications supply chain, industry needs more than databases like the MITRE Corporation's Common Vulnerabilities and Exposures.[17] There is no centralized risk registry for companies with suspected ties to foreign adversaries or lists of dubious manufacturers or software developers. In the telecommunications industry, such information is gleaned on an ad hoc basis, such as through government contract negotiations or by inferences

[15] One example–the controversial Bloomberg article about Super Micro and the alleged hack of its hardware–illustrates some of the challenges in parsing the sensational from the credible in assessing security threats. *See* Jordan Roberston and Michael Riley, *The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies*, Bloomberg Businessweek (Oct. 4, 2018), https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies; Cailtin Cimpanu, *Super Micro trashes Bloomberg chip hack story in recent customer letter*, ZDNet (Oct. 23, 2018), https://www.zdnet.com/article/super-micro-trashes-bloomberg-chip-hack-story-in-recent-customer-letter/.

[16] DHS, Binding Operational Directive 17-01 (Sept. 13, 2017), https://cyber.dhs.gov/bod/17-01/.

[17] MITRE, Common Vulnerabilities and Exposures, https://cve.mitre.org/ (last visited July 26, 2020).

from Team Telecom interactions.

"[L]ong-vexing [Information and Communications Technology ("ICT")] supply chain risk challenges" will not easily be resolved.[18] NTIA can see this in other government efforts to secure supply chains. Section 889 of the FY2019 National Defense Authorization Act has raised concerns about the overbreadth and impracticality of its attempt to impose prohibitions that might reach global supply chains.[19] The Federal Acquisition Supply Council has faced complex concerns about effective blacklisting and how to communicate information. The Department of Commerce's implementation of the Executive Order on Securing the Information and Communications Technology Supply Chain ("Executive Order No. 13873") drew substantial concern about its breadth, administrability, and possible overseas application.[20] NTIA should consider the congressional mandate in Section 8 of the Act against this backdrop and look for ways to improve information sharing. And it should do this at Phase One, and not just at Phase Two.

C. Numerous venues exist for the government to share information with the communications sector including DHS and the Communications Sector Coordinating Council.

NTIA should implement Section 8 by encouraging expansion of existing information sharing programs that are already being facilitated by other federal agencies. Respectfully, this suggests that the Phase One implementation of C–SCRIP described in the July 8 Notice may not

[18] CISA, Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, at 25 (Sept. 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.

[19] National Defense Authorization Act for Fiscal Year 2019, H.R. 5515, 115th Cong., div. A, § 889 (as passed in House on May 24, 2018 by a recorded vote of 351-66), https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515rh.pdf; *see also* Defending Government Communications Act, H.R. 4747, 115th Cong. (2018), https://www.congress.gov/115/bills/hr4747/BILLS-115hr4747ih.pdf; S. 2391, 115th Cong. (2018) (Senate companion to H.R. 4747) ("*FY2019 NDAA*").

[20] Dep't of Commerce, Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 65316 (Nov. 27, 2019), https://www.govinfo.gov/content/pkg/FR-2019-11-27/pdf/2019-25554.pdf; Exec. Order No. 13873, 84 Fed. Reg. 22689 (May 15, 2019) ("Executive Order No. 13873").

be the right path forward, particularly to the extent the endeavor is in addition to existing information sharing efforts. The July 8 Notice states that its "strategic implementation plan is intended to harmonize the C–SCRIP program with other government programs to ensure cohesion and to avoid overlap;" but this requires public comment and input on the venues that work and development of the foundational plan should include industry stakeholders.[21]

DHS is the sector specific agency for telecommunications and its cybersecurity functions were recently reordered and codified into a new agency, the Cybersecurity and Infrastructure Security Agency ("CISA"). DHS has been identified in statute, practice, and recent recommendations as the key focal point for communication with the communications sector.[22] Phase One in NTIA's July 8 Notice includes DHS, as well as ODNI, FBI and the FCC, as directed by Congress. NTIA should consider how to ensure that such a broad group, including the presence of a regulator in the FCC, does not muddle the functions of any C–SCRIP or successor.

DHS has focused on 5G security and supply chain management. Its ICT Supply Chain Risk Management ("SCRM") Task Force ("DHS ICT Task Force") has multiple workstreams underway,[23] including the work of the Task Force's Working Group 1, which is examining information sharing with an emphasis on actionable, bi-directional information sharing. CISA has also been working with other agencies to develop a legal framework for the assessment of supply chain risks, including on the government-wide implementation of Executive Order No.

[21] *See July 8 Notice* at 41006 (describing the importance of the implementation plan).
[22] CSRIC V, Working Group 5: Cyber Security Information Sharing, Final Report, 4 (Mar. 2017), https://www.fcc.gov/files/csric5-wg5-finalreport031517pdf (noting "DHS is leading in government information sharing with the private sector") ("*CSRIC V Working Group 5 March 2017 Report*").
[23] *Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force*, CISA (last revised June 15, 2020), https://www.cisa.gov/ict-scrm-task-force.

13873, as well as on agency-specific initiatives, such as FCC's Universal Service Fund ("USF") Supply Chain proceedings.

The Critical Infrastructure Partnership Advisory Council ("CIPAC") is a DHS-chartered advisory council that provides a forum that enables members of the recognized government coordinating councils ("GCCs") and sector coordinating councils ("SCCs") to discuss joint critical infrastructure matters for the purpose of achieving consensus on policy, advice, and recommendations to be presented to the Federal government.

The Communications Sector Coordinating Council ("CSCC") is a vital venue for industry collaboration on security. The CSCC meets regularly to review industry and government actions on critical infrastructure protection priorities and cross sector issues. The CSCC coordinates with industry participants in the NSTAC and the Communications-Information Sharing and Analysis Center ("NCCIC"). The CSCC was chartered in 2005 to help coordinate initiatives on physical and cyber security of sector assets and "to ease the flow of information within the sector, across sectors and with designated Federal agencies."[24]

The FCC's CSRIC is another venue that can facilitate information sharing between government and the private sector. For decades, the CSRIC has brought together public and private sector experts to address technical and operational issues, including those relating specifically to information sharing in the sector,[25] as well as recommendations on supply chain.[26]

Industry groups, like the CTIA Cybersecurity Working Group, are actively engaged in seeking and sharing information about supply chain and other government priorities, regularly

[24] *About the CSCC*, US Communications Sector Coordinating Council, https://www.comms-scc.org/about-1 (last visited July 26, 2020).
[25] *CSRIC V Working Group 5 March 2017 Report*.
[26] CSRIC VI, Working Group 3: Network Reliability and Security Risk Reduction, Addendum to Final Report (Sept. 2018), https://www.fcc.gov/file/14855/download.

inviting DHS, NIST, and others to its bi-weekly meetings. The government should seek out opportunities to participate in these industry efforts, provide additional forums for increased government-industry exchange, and encourage small and rural providers to participate as well.

III. NTIA SHOULD PROMOTE THE DISSEMINATION OF ACTIONABLE INFORMATION TO A BROAD SET OF INDUSTRY RECIPIENTS

A. "Supply chain risk" should be defined to maximize timely, actionable information sharing and minimize geopolitical or economic information.

To have the biggest impact, NTIA should not go beyond the statute's focus on "supply chain security risk,"[27] to include, as it proposes, "broader strategic risks to the U.S. economy and national security, including risks to the global 5G market"[28] and the goals of the National Strategy to Secure 5G.[29] NTIA says that "[d]efining 'supply chain security risk' to encompass national security and economic risk will reinforce the Act's purpose to safeguard the economy and national critical infrastructure against these risks."[30] However, CTIA and its members with vast experience in information sharing and telecommunications supply chain decisions, urge NTIA to focus on verified, actionable information about supply chain security risk and de-emphasize geopolitical and macro-economic issues. Many providers struggle to resource an internal security team that can ingest indicators of compromise or evaluate supply chain risks; it is unrealistic to expect them to dedicate resources to consider geopolitical issues or the government's desire to promote global vendor diversity. Including such information may

[27] *See RFC* at 35920; *July 8 Notice* at 41006. NTIA plans to use the Federal Acquisition Supply Chain Security Act of 2018, 41 U.S.C. §§ 1321-28, which defines "supply chain risk" by reference to 41 U.S.C. § 4713: "the risk that any person may sabotage, maliciously introduce unwanted function, extract data, or otherwise manipulate the design, integrity, manufacturing, production, distribution, installation, operation, maintenance, disposition, or retirement of covered articles so as to surveil, deny, disrupt, or otherwise manipulate the function, use, or operation of covered articles or information stored or transmitted on the covered articles."
[28] *RFC* at 35920.
[29] White House, National Strategy to Secure 5G of the United States (Mar. 2020), https://www.whitehouse.gov/wp-content/uploads/2020/03/National-Strategy-5G-Final.pdf.
[30] *RFC* at 35920.

undermine the utility, clarity, and credibility of information shared and reduce the likelihood that it is used.

NTIA asks if there are supply chain security risks beyond those Congress specified that should be included in an information security program, and what sorts of risks and vulnerabilities should be covered by the language "specific risk and vulnerability information related to equipment and software."[31] As the DHS ICT Task Force previously noted, useful information includes "identified product-based risks such as counterfeit products, device impersonation, and malicious code insertion. It may also include organizational risks, such as insider threat activities and physical attacks against participants or products in the supply chain."[32] Risk information could relate to software vulnerabilities, suspected malware, hardware concerns, compromise of manufacturing facilities, indications of problems in the security of updates and patches, or other security concerns. The key for any information sharing is that it be verified, timely, and actionable.

B. NTIA should not adopt a rigid approach to determine whether companies are "trusted."

The Act contemplates information sharing with "trusted" providers and suppliers – entities "not owned by, controlled by, or subject to the influence of a foreign adversary."[33] CTIA supports the government focusing on untrustworthiness by reference to control by a foreign

[31] *Id*. at 35921.
[32] CISA, Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report, at 14 (Sept. 2019), https://www.cisa.gov/sites/default/files/publications/ICT%20Supply%20Chain%20Risk%20Management%20Task%20Force%20Interim%20Report%20%28FINAL%29_508.pdf.
[33] Secure and Trusted Communications Networks Act §8(c)(4). NTIA indicates that "ineligible providers and suppliers will be determined by: (1) any executive branch interagency body with appropriate national security expertise, including the Federal Acquisition Security Council; (2) the Department of Commerce pursuant to Executive Order No. 13873; (3) the equipment or service being covered is telecommunications equipment or services, as defined in section 889(f)(3) 2019 NDAA, or (4) an appropriate national security agency." *RFC* at 35920.

adversary, rather than trying to establish detailed criteria for a company to be considered "trusted." NTIA should be wary of over-reliance on the country of corporate parentage, which can keep U.S. subsidiaries out of other federal programs, such as in the trade policy area.

The concept of "foreign adversary"[34] should offer predictability but need not be rigidly defined for purposes of determining who can receive threat information. NTIA appropriately plans to fluidly use the determinations of the Federal Acquisition Council, Executive Order No. 13873, Section 889 of the FY2019 NDAA, and appropriate expert agencies. However, as CTIA and numerous commenters told the Department of Commerce during the implementing proceeding for Executive Order No. 13873, the private sector needs a level of regulatory certainty about what entities the government considers "foreign adversaries" in order to structure transactions. The need for clarity in that context is acute, because it determines the legality of transactions and investments, thereby having direct and substantial effects. However, because no entity is entitled to receive sensitive government information, NTIA can take a flexible approach to "trusted" provider and need not adopt the exact same definition as the Department of Commerce in implementing Executive Order No. 13873.

C. A broad approach to eligibility will promote robust participation.

In directing NTIA to tackle information sharing, Congress rightly recognized that smaller and rural providers need better access to information from the government, to avoid sunk costs from investments in equipment that the government may come to believe are a threat to national security. An unduly narrow approach would be counter to the increasing emphasis across government on information sharing and partnerships with the government. NIST's seminal

[34] *See* Secure and Trusted Communications Networks Act.

Cybersecurity Framework added information sharing expectations, and the Cyberspace Solarium Commission recently made recommendations for enhanced information sharing.[35] The July 8 Notice of the C–SCRIP appears to prejudge some of the eligibility questions posed in the RFC. CTIA urges NTIA to take a broad approach to eligibility because a rigid or narrow approach risks creating fragmentation and undermining information sharing. The July 8 Notice seems to move in the wrong direction by suggesting that NTIA has already opted for a more narrow approach. NTIA should be careful to not make threshold decisions before all stakeholders have had the opportunity to weigh in.

Similarly, too narrow an approach to "advanced communications services" may constrain information sharing. The Act directs NTIA to share risk information with trusted providers of "advanced communications service," which the legislation equates with "advanced telecommunications capability" as defined in section 706 of the Telecommunications Act of 1996. NTIA should not limit itself to the FCC's regulatory benchmarks for "advanced" communications services[36] when determining which providers to share information with. Given the disparate deployment of services across the country, NTIA's sharing efforts should be inclusive in order to garner the most value; it should not apply criteria adopted by the FCC for primarily regulatory purposes. Regulatory thresholds may change, and it may be providers migrating from 3G to 4G, or otherwise looking to improve, that are most in need of information.

[35] *See e.g.*, NIST, Framework for Securing Critical Infrastructure Cybersecurity Version 1.1 (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; Solarium Commission Recommendations at Recommendations 4.6.1, 5.1.1, 5.2, 6.2.1.

[36] NTIA notes that "for mobile services, the FCC has determined that 4G Long Term Evolution services offering transmission speeds between 5Mbps/1Mbps and 10Mbps/3Mbps are the 'best proxy' for advanced mobile service." *RFC* at 35921 (citation omitted).

NTIA should also decline to import the 2 million customer limit from the Act's "remove and replace" reimbursement program.[37] The goals of information-sharing in Section 8 are fundamentally different from the need to limit eligibility for scarce funding. CTIA encourages NTIA avoid a rigid approach, lest it fragment and undermine information sharing.

IV. NTIA SHOULD CONSIDER THE IMPACT ON SMALL AND RURAL PROVIDERS, PROMOTING STREAMLINED USE OF EXISTING PROCEDURES TO MINIMIZE INFORMATION SHARING BURDENS

A. Existing venues, like the DHS ICT Task Force and the CSCC, can help disseminate information to small and rural providers.

CTIA appreciates NTIA's desire "to avoid the re-creation of existing threat and vulnerability information sharing programs" and urges NTIA to work with its government counterparts to de-conflict and to take advantage of programs that already exist.[38] As CSRIC observed long ago "[a] critical organizational challenge facing the communications sector is the wide variety of private, public, public-private, and international groups, entities, and arrangements devoted to cyber threat information sharing."[39] Adding supply chain into the mix risks further complicating these challenges.

Accordingly, NTIA should focus on the work of existing venues, as described above, particularly the CSCC and the DHS ICT Task Force, to make more information available to more providers and suppliers. NTIA should work with these existing fora to centralize and coordinate points of contact and data flows to minimize the number of memberships smaller operators need to participate in or monitor.

Small and rural providers should be encouraged to join existing venues, perhaps in

[37] *Id.* at 35921.
[38] *Id*.
[39] *CSRIC V Working Group 5 June 2016 Report* at 2.

working groups that focus on their needs. The DHS ICT Task Force and the respective Working Groups recognized "the unique circumstances and needs of small and medium-sized businesses" and has already had opportunities to "address concerns and needs of small and medium-sized businesses operating within the ICT supply chain ecosystem."[40] It should be encouraged to delve deeper with greater small and rural provider participation.

The CSCC costs nothing to join, making it an ideal forum to convey information from NTIA to private sector members, especially small and rural providers. NTIA could consider working with the CSCC to focus on the needs of small and rural providers and how best to tailor the conveyance of information to them. NTIA should dedicate resources to broadening participation in these efforts and avoid creating a separate workstream that may make it harder for smaller carriers to interface with the government—the fewer bodies small and rural operators need to join in order to obtain information, the better.

B. In considering barriers and how to share information, NTIA needs to be realistic about how companies receive and process security risk information.

NTIA asks about barriers that small and rural providers and suppliers face in accessing security risk information from non-government sources and what the Federal government can do to eliminate or mitigate those barriers.[41] As discussed above, information is available from various sources, but it is often hard to validate even for the largest operators, making it nearly impossible for smaller and more rural operators to manage.

Large telecommunications providers and suppliers have robust risk management programs that take advantage of varied sources of information, including third-party assessments

[40] *CISA's ICT Supply Chain Risk Management Task Force Approves New Working Group For Second Phase*, CISA (Dec. 18, 2019), https://www.cisa.gov/news/2019/12/18/cisas-ict-supply-chain-risk-management-task-force-approves-new-working-group-second.
[41] *RFC* at 35922.

and consultants. These sorts of programs may not be economical or necessary for each small provider, making it more important that the government and relevant associations are able to disseminate actionable information to these operators on a timely basis.

In terms of NTIA's interest in how specific security risk information needs to be to help companies make procurement decisions, it will vary. CSRIC has observed that when information is shared, "[c]ontextual data is often missing, e.g., an IP is listed as bad, but there's no further information as to why it is bad or how an ISP can determine whether a detection is a false positive."[42] It is imperative that information the government is sharing be actionable, and that will require a certain amount of context.

The utility of information is a function of timing, as much as specificity. Whether information is actionable in the context of the operator's business will depend on when it arrives and what aspect of the business it impacts. In the area of threat mitigation and response, specific indicators of compromise ("IOCs") are helpful and actionable in daily operations to protect networks, while information pertaining to supply chain risk may be relevant to significant long-term decisions that happen less frequently. Information that impacts procurement will depend on when during the purchase cycle it is received—purchases of core network equipment are more rare and larger; decisions about what end user devices to offer and support may be made more frequently—but each will have substantial impacts on business planning. In light ot these dynamics, generic information may not be actionable or may not come at the right time relative to a decision. So, information sharing efforts need to offer both "unclassified information through typical civilian channels (for example, by e-mail)" and the option to "receive more detailed classified information that would require a staff member to obtain a security clearance

[42] *CSRIC V Working Group 5 June 2016 Report* at 10.

and could require travel to receive the classified information in person at a secure location."[43]

NTIA asks whether there are "legal barriers that could impede the ability of trusted providers and suppliers to receive or act on security risk information from the Federal government."[44] Barriers are likely to be more practical and operational than legal, though certainly information from the government that suggests the need to terminate a relationship could have contractual implications. To address potential unease about participating in information sharing, the government can confirm that there is no obligation to participate in or continue participating in information sharing programs. NTIA should make clear, as in CISA, that the receipt of risk information from the government creates no duty, implied or otherwise, to act; that a 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.

C. Alternative approaches, such as company-requested risk and vulnerability information, may help small and rural providers evaluate supply chain decisions.

NTIA asks if eligible providers and suppliers should have an opportunity to request risk and vulnerability information about specific equipment, software, and services.[45] For smaller and rural providers this may be a welcome addition to information sharing with the government, as it reduces their overall burdens to constantly monitor information flows and manage supply chain risks, while permitting them to solicit information at times that are relevant and timely for their specific procurement decisions. Such a function would need to keep requests confidential, as equipment and supply chain decisions are typically highly confidential and proprietary, but some providers may prefer the ability to come to DHS or another government agency and seek

[43] *RFC* at 35922.
[44] *Id.*
[45] *Id.* at 35921.

specific guidance on contemplated purchases or partnerships. However, NTIA should ensure that any such option does not promote a government pre-approval regime or expectation.

V. DECLASSIFICATION AND SECURITY CLEARANCES SHOULD BE PRIORITIZED FOR THE ENTIRE TELECOMMUNICATION SECTOR

NTIA asks if small and rural providers and suppliers have encountered problems in attempting to obtain security clearances, and if so, what has been the nature of those difficulties.[46] Across the industry, everyone from small to large providers have encountered slow review. This is an area that warrants immediate and aggressive attention, as has been called for over many years by CSRIC, NSTAC, and other groups.

NTIA asks what means of sharing information best balances the objectives of the Act and the need to safeguard sensitive information.[47] This will be a combination of activities, some in the form of disseminating actionable de-classified information to identified 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 information without the need to bring a company employee to a Sensitive Compartmented Information Facility ("SCIF") or have a cleared representative. In general, providers confront delays or overly burdensome demands to obtain clearances, in relation to the information to be shared. The onus should be on the government to find a less burdensome path forward.

These issues should not await even more study and review, as contemplated by the Solarium Commission Recommendations and many others. As a Council on Foreign Relations

[46] *Id*. at 35922.
[47] *Id*. at 35921.

report recommended, the government should "[r]evamp security clearance rules. The Secretary of Homeland Security should accelerate efforts to write rules granting clearances to non-defense companies, which have languished since 2015."[48]

VI. NTIA SHOULD SEIZE ON ITS COORDINATING ROLE TO PROMOTE HARMONIZATION OF DISPARATE SUPPLY CHAIN EFFORTS

NTIA is an ideal convener of inter-agency work on supply chain security. As CTIA and many others have told the Department of Commerce, the multiplicity of supply chain security efforts underway is untenable. The significant fragmentation and overlap of efforts is taxing to the resources of even the larger companies that have the staff to directly engage in all these proceedings. However, the same is not true for all members of the industry, particularly the smaller and more rural members. Supply chain efforts should be harmonized and streamlined, not just for the purposes of developing the regulations but also for the long-term execution of these objectives.

VII. CONCLUSION

Information sharing is one of the most important ways to advance security. NTIA has a unique opportunity to help resolve lingering issues, harmonize workstreams, and expand information sharing. CTIA looks forward to working with NTIA on these and its other goals as the nation moves to a 5G future.

[48] Robert K. Knake, *Sharing Classified Cyber Threat Information With the Private Sector*, Council on Foreign Relations (May 15, 2018), https://www.cfr.org/report/sharing-classified-cyber-threat-information-private-sector.

Respectfully submitted,

/s/ Melanie K. Tiano
Melanie K. Tiano
Director, Cybersecurity and Privacy

Thomas K. Sawanobori
Senior Vice President and Chief Technology Officer

John A. Marinho
Vice President, Technology and Cybersecurity

CTIA
1400 16th Street, NW, Suite 600
Washington, DC 20036
202-736-3200
www.ctia.org

July 28, 2020