Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers	)	Docket No. 200609-0154

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
(CompTIA)

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION (CompTIA)
322 4th Street NE
Washington, DC 20002

July 28, 2020

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY 1

I. FOCUSING ON SMALL AND RURAL PROVIDERS IS APPROPRIATE, BUT SUPPLIERS OF ALL SIZES ALSO NEED ACCESS TO RELEVANT RISK INFORMATION. 2

A. Focusing on Small and Rural Providers is Appropriate, but Small Suppliers Should Not Be Overlooked. 3

B. Trusted Suppliers of All Sizes Need Access to Threat Information to Effectively Manage Risk Throughout Supply Chains. 5

II. KEY TERMS SHOULD BE DEFINED TO MAXIMIZE PARTICIPATION, INFORMATION FLOW, AND CERTAINTY. 6

A. The Term "Supply Chain Security Risk Information" Should Be Construed Broadly While the Program Is Being Established. 6

B. The Term "Trusted Providers and Suppliers" Must Be Construed Broadly but Still Provide Paths to Promote Sensitive Information Sharing. 8

C. The Term "Foreign Adversary" Must Be Clarified Before It Can Be Used. 10

D. The Terms "Advanced Communications Service" and "Communications Equipment or Services" Should Be Construed as Broadly as Reasonably Possible. 11

III. THE INFORMATION SHARING PROGRAM SHOULD INCLUDE BOTH "PUSH" AND "PULL" ELEMENTS. 14

CONCLUSION 16

Before the
NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
Washington, DC 20230

In the Matter of	)	
	)	
Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers	)	Docket No. 200609-0154

COMMENTS OF
THE COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION
(CompTIA)

The Computing Technology Industry Association ("CompTIA"),[1] the leading association for the global information technology (IT) industry, respectfully submits these comments to the National Telecommunications and Information Administration ("NTIA") in response to the above-captioned Request for Comments ("RFC").[2]

INTRODUCTION AND SUMMARY

CompTIA appreciates the Administration's work toward implementing Section 8 of the Secure and Trusted Communications Network Act ("Secure Networks Act"), which requires the development of a supply chain security risk information sharing program.[3] Information sharing is a meaningful and practical path toward enhancing the security of communications network supply chains, and the Section 8 program holds significant promise toward advancing these

[1] CompTIA supports policies that enable the information technology industry to thrive in the global marketplace. We work to promote investment and innovation, market access, robust cybersecurity solutions, commonsense privacy policies, streamlined procurement, and a skilled IT workforce. Visit www.comptia.org/advocacy to learn more.

[2] NTIA, *Promoting the Sharing of Supply Chain Security Risk Information Between Government and Communications Providers and Suppliers*, RIN 0660-XC046, 85 Fed. Reg. 35919 (June 12, 2020) ("RFC").

[3] Pub. L. No. 116-124 § 8, 134 Stat. 158, 168 (Mar. 12, 2020) (codified at 47 U.S.C. § 1607).

goals. NTIA formally announced the establishment of the Communications Supply Chain Risk Information Partnership ("C-SCRIP") on July 8, 2020 in furtherance of Section 8, and we welcome this opportunity to provide input regarding the development of this new program.[4]

The RFC appropriately focuses on small providers and suppliers, which makes sense based on the circumstances that led to the enactment of the Secure Networks Act in the first place. However, additional attention should be given to issues specific to small *suppliers*, and trusted suppliers of all sizes should be eligible to participate given that they provide products and services to small providers. In accordance with both the text and underlying objectives of the Secure Networks Act, terms like "supply chain risk" and "trusted supplier" should be defined broadly to avoid pre-emptively limiting the type of information shared, and to maximize participation while still providing paths to promote the sharing of sensitive information. Finally, both "push" and "pull" approaches to information sharing should be used so that companies have access to information at the time when they are making purchasing decisions.

DISCUSSION

I. FOCUSING ON SMALL AND RURAL PROVIDERS IS APPROPRIATE, BUT SUPPLIERS OF ALL SIZES ALSO NEED ACCESS TO RELEVANT RISK INFORMATION.

The RFC notes that "[a]lthough the Act mentions small and rural providers and suppliers only in the context of engagements with the Federal government, NTIA believes those entities should be the principal focus of the information sharing program."[5] This is generally the right approach, although as explained below NTIA must specifically consider small *suppliers* as well as small providers. In addition, trusted suppliers of *all* sizes must also be able to participate in

[4] NTIA, *Establishment of the Communications Supply Chain Risk Information Partnership*, 85 Fed. Reg. 41006 (July 8, 2020) ("C-SCRIP Establishment Notice").

[5] RFC, 85 Fed. Reg. at 35921 (columns 2-3).

the program if it is to be effective in serving the needs of the small providers who are their customers.

A. Focusing on Small and Rural Providers is Appropriate, but Small Suppliers Should Not Be Overlooked.

Small providers. The Secure Networks Act is primarily intended to "prohibit certain Federal subsidies from being used to purchase communications equipment or services posing national security risks" and "to provide for the establishment of a reimbursement program for the replacement of communications equipment or services posing such risks."[6] Section 8 of the Act, entitled "NTIA program for preventing future vulnerabilities," implies that the first seven sections of the law are intended to prevent current vulnerabilities while Section 8 is intended to prevent the same kinds of vulnerabilities from reoccurring in the future.

The RFC aptly recognizes that in directing the FCC to establish a program reimbursing smaller providers for removing and replacing equipment and services from suppliers of concern, Congress did so partially "because it believed that smaller providers did not receive a sufficient 'heads-up by our government'" about the national security risks.[7] Moreover, the RFC rightly observes that Section 8 was intended to "fix this information gap by ensuring that [small, rural providers] have access to the information they need to keep their networks and Americans secure."[8] Under these circumstances, it is entirely appropriate for NTIA to focus the program on providing small and rural communications providers with information that will help them better manage risks to their supply chains.

---

[6] Secure Networks Act (long title of law), 134 Stat. 158.

[7] RFC, 85 Fed. Reg. at 35921 (column 3) (quoting remarks of Rep. Doyle).

[8] *Id.* (quoting remarks of Rep. Latta).

Small suppliers. The Act makes clear that "*suppliers* that … are small businesses" should also receive heightened engagement.[9] Accordingly, in explaining the intended "principal focus" of the program, the RFC correctly includes both small and rural "providers and suppliers," although suppliers are mentioned only in passing after the more significant discussion of small providers (see above) that motivated enactment of the Act.[10]

The inclusion of small suppliers is not merely a quirk in the law. Just as small *providers* can benefit from information that may affect their equipment purchase decisions, so too can small *suppliers* – who have both large and small customers – benefit from information regarding their upstream supply chains. This should be an intentional area of focus, not merely something ancillary to the focus on small service providers. The C-SCRIP Establishment Notice issued on July 8th does not include suppliers in Phase 1 of the program, and while suppliers are briefly mentioned in Phase 2, the Notice states that NTIA will only "initiate ad hoc briefings to trusted providers," not suppliers.[11] This is concerning and gives the impression that the importance of early and sustained engagement with suppliers of all sizes is being overlooked.

Size threshold for small suppliers. Acknowledging the importance of small suppliers for heightened engagement and program evaluation purposes may also require establishing a size threshold – an issue the RFC does not squarely address. To be sure, the Act places a cap of 2 million customers on defining eligibility for the "remove and replace" program, and this may be an appropriate threshold for determining small business *provider* engagement. However, an

[9] Secure Networks Act § 8(a)(2)(B)(i).

[10] RFC, 85 Fed. Reg. at 35921 (column 3).

[11] C-SCRIP Establishment Notice, 85 Fed. Reg. at 41006.

individual number of customers is ill-suited to determining whether a *supplier* is a small business, and whether a sufficient number of smaller suppliers are engaged in the program.

Better measures for small suppliers may be found in Small Business Administration ("SBA") definitions of "small business." For example, a company engaged in "radio and television broadcasting and wireless communications equipment manufacturing" is a small business if it has 1,250 or fewer employees, and a company engaged in "other communications equipment manufacturing" is a small business if it has 750 or fewer employees.[12] Since "suppliers" in this context could also include software-based or service-based alternatives, a somewhat more expansive and uniform definition – perhaps either up to 1,500 employees or up to $40 million in average annual receipts, both common thresholds used by the SBA across many categories – could potentially be used here for the sake of simplicity.

B. Trusted Suppliers of All Sizes Need Access to Threat Information to Effectively Manage Risk Throughout Supply Chains.

Small service providers routinely purchase equipment from suppliers of all sizes; indeed, the government is well aware that many of the alternatives to the covered equipment being replaced under the Act would be provided by large suppliers. Thus, while it is appropriate to tailor the program to meet the information sharing needs of small businesses, trusted vendors of all sizes that supply ICT equipment and services to small and rural providers must also be able to access information shared through the program in order to effectively manage risk to those networks.

---

[12] SBA, *Table of Small Business Size Standards Matched to North American Industry Classification System Codes*, at 17 (NAICS Codes 334220 & 334290), https://www.sba.gov/sites/default/files/2019-08/SBA%20Table%20of%20Size%20Standards_Effective%20Aug%2019%2C%202019.pdf.

Moreover, supply chain risk management requires the ability to communicate risk and responsibilities throughout the value chain. If small and rural providers are expected to make purchasing decisions based on information shared by NTIA, they need to be able to share that information with their trusted vendors so that those vendors can make decisions accordingly. Thus, it would serve the goals of the Act to permit trusted suppliers of all sizes to participate fully in the information sharing program. In addition, while business size thresholds may be useful to measure the effectiveness of NTIA's efforts to *engage* small suppliers, *see* section I-A above, imposing artificial size limits on supplier *participation* would therefore be inappropriate and counterproductive.

II. KEY TERMS SHOULD BE DEFINED TO MAXIMIZE PARTICIPATION, INFORMATION FLOW, AND CERTAINTY.

While appropriate to target the information sharing program to serve small providers and their suppliers, the bounds of participation should nevertheless remain broad in order to maximize the effectiveness of the information shared. As such, the terms "supply chain security risk information," "trusted providers and suppliers," "advanced communications service," and "communications equipment or service" should be construed broadly, while the term "foreign adversary" must be clarified before it can be effectively used.

A. The Term "Supply Chain Security Risk Information" Should Be Construed Broadly While the Program Is Being Established.

CompTIA supports some general reliance on the broad definition of "supply chain risk" provided by the 2018 Federal Acquisition Supply Chain Security Act, as contemplated by the RFC.[13] However, we discourage NTIA from arbitrarily scoping the term "supply chain security

[13] RFC, 85 Fed. Reg. at 35920 (columns 2-3); 41 U.S.C. § 4713(k)(6) (added by Federal Acquisition Supply Chain Security Act, Pub. L. No. 115-390, title II, § 203, 132 Stat. 5173, 5192).

risk" too specifically at the outset of the program. Rather, NTIA should tailor what kinds of supply chain security risk information are shared over time as industry and government evolve in their understanding of what information is most valuable to providers and suppliers. For example, the Information Sharing Working Group in the DHS ICT Supply Chain Risk Management ("SCRM") Task Force found in its Year One effort that the ability to share names of specific suppliers and ecosystem participants of concern was highly valuable information to private entities trying to manage risk, but that various legal challenges often discouraged such information sharing.[14] The working group is currently exploring ways to reduce those barriers when it is appropriate to share such information between private entities.

While the ability to identify and share the names of bad actors, particularly with one's suppliers, is still a critical aspect of information sharing from government to industry, other kinds of information may eventually supersede that type of information in terms of unique value. For example, information about more general supply chain threats or the vulnerability of specific types of products – rather than specific manufacturers – may eventually prove as much or more useful than sharing the names of specific companies of concern. Thus, NTIA's information sharing program should retain as much flexibility as possible when defining the kinds of supply chain information shared.

Similarly, technological advancement may enhance the ecosystem's ability to collect, aggregate, share, analyze, and use risk information over time and the program should remain flexible enough to adopt those practices as they become available and are deemed helpful. CompTIA appreciates recognition in the RFC of the ICT SCRM Task Force's important work on

[14] Cybersecurity and Infrastructure Security Agency, *Information and Communications Technology Supply Chain Risk Management Task Force: Interim Report*, September 2019, at 14-15.

this issue, and CompTIA actively participates in the Task Force. NTIA should continue to leverage the unique expertise and insight of the ICT SCRM Task Force and engage in ongoing discussion to further scope the term "supply chain security risk information" in practice without adopting or codifying a narrower definition.

B. The Term "Trusted Providers and Suppliers" Must Be Construed Broadly but Still Provide Paths to Promote Sensitive Information Sharing.

CompTIA likewise urges NTIA to take an inclusive approach regarding the term "trusted providers and suppliers." The statutory definition of the term "trusted" is fairly broad and includes any entity that is "not owned by, controlled by, or subject to the influence of a foreign adversary."[15] NTIA is therefore correct to include any provider or supplier NOT specifically deemed ineligible by Section 2(c) of the Act.

At least for purposes of basic participation in this program, NTIA thus need not and may not create a separate "qualified list" of trusted providers and suppliers. As CompTIA has noted in related contexts and the DHS ICT SCRM Task Force's working group on Qualified Bidder/Manufacturer Lists has discussed at length, qualified lists tend to be very resource intensive and if not carefully tailored and maintained to serve a discrete mission, can introduce a variety of legal, security, and functional risks.[16] The marginal benefit to NTIA's ability to share information gained by thoroughly vetting and qualifying small providers and suppliers for participation would be far outweighed by the cost of structuring the program to rely on that process. Furthermore, the bounds of defining ineligible participants in the legislation itself

[15] Secure Networks Act § 8(c)(4).

[16] *See* CompTIA Comments on *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Programs*, WC Docket No. 18-89, May 20, 2020, at 3-8.

implies that any entity not meeting the criteria of untrusted supplier should be eligible to participate in the information sharing program.

A broad list of eligible participants might be viewed as limiting the amount of highly valuable or very sensitive information that could be shared with *all* participants. However, since the primary concern to date has related to specific suppliers of concern, it may be possible for NTIA to facilitate limited-purpose clearances for sharing that type of information with certain individuals based on their positions, especially for small and rural businesses and suppliers that are often thinly-staffed. Sub-classified designations such as For Official Use Only (FOUO), Protected Critical Infrastructure Information (PCII), or Sensitive Security Information (SSI) may provide useful frameworks from which to draw to facilitate the information sharing, ideally without the burden and expense of a full security clearance.[17]

Meanwhile, NTIA could still provide the most sensitive information to those participants who are cleared at the TS/SCI level. This would allow NTIA to build a conduit of supply chain security risk information wherein the agency could share more sensitive/valuable information without having to build its own list. The process comes with some downsides as it would be more resource-intensive and may disproportionately advantage large companies over smaller ones, which creates some tension with other goals of the Secure Networks Act. Even so, such an approach could facilitate better information sharing that would help mitigate risk across the nation's networks. Ultimately, NTIA will need to balance these interests without letting the perfect be the enemy of the good.

[17] *See e.g.*, Dep't. of Homeland Security, Management Directive System, MD No. 11042.1, *Safeguarding Sensitive but Unclassified (For Official Use Only) Information*, Jan. 6, 2005.

C. The Term "Foreign Adversary" Must Be Clarified Before It Can Be Used.

NTIA is right to keep its designations of "foreign adversaries" consistent with decisions of the Secretary of Commerce under EO 13873, particularly since the Secure Networks Act uses identical language. However, as CompTIA noted in comments to the Department of Commerce in January 2020 regarding implementation of EO 13873, greater clarity is needed regarding the term "foreign adversary."[18] In order to use this term effectively, consistent with due process, the Department should develop a set of criteria that can be used as a transparent guide, focusing on entities, not whole countries. Alternatively, if the Department adopts a country-focused approach and does not provide an exact list of which countries it considers to be foreign adversaries, it can provide some greater clarity by incorporating terms such as "mutual defense treaty allies" and "strategic partners" of the United States.

Meanwhile, on May 1, 2020 the President issued an executive order on securing U.S. bulk-power systems (EO 13920) that is similar in purpose and structure to EO 13873.[19] The bulk-power executive order also uses the term "foreign adversary" and the Department of Energy ("DOE") elaborated on that term in a Request for Information ("RFI") published on July 8.[20] The DOE RFI states that "[t]he current list of 'foreign adversaries' consists of the governments of" China, Cuba, Iran, North Korea, Russia, and Venezuela, but makes clear that this list is for purposes of EO 13920 only.[21] If the Department of Commerce pursues a country-specific

---

[18] CompTIA Comments on *Securing the Information and Communications Technology and Services Supply Chain*, Docket No. DOC-2019-0005 (Jan. 10, 2020) at 21-22.

[19] Exec. Order No. 13920, 85 Fed. Reg. 26595 (May 1. 2020).

[20] Dep't. of Energy, *Securing the United States Bulk-Power System*, 85 Fed. Reg. 41023, 41024 (July 8, 2020).

[21] *Id.*

approach to the question of "foreign adversaries," it should consider harmonizing its approach with that taken by DOE.

D. The Terms "Advanced Communications Service" and "Communications Equipment or Services" Should Be Construed as Broadly as Reasonably Possible.

Under the Secure Networks Act, participation in the information sharing program is open to trusted providers of "advanced communications services" and to trusted suppliers of "communications equipment and services."[22] The Secure Networks Act defines the term "advanced communications services" as being equivalent to "advanced telecommunications capability," which is further defined in Section 706 of the Telecommunications Act of 1996, "without regard to any transmission media or technology, as high-speed, switched, broadband telecommunications capability that enables users to originate and receive high-quality voice, data, graphics, and video telecommunications using any technology."[23]

Viewed from a provider lens, the term "advanced communications service" should be construed broadly to include most broadband services, thus making all or nearly all service providers eligible. The FCC has just proposed to define the term based on a connection speed of just *200 kbps in either direction*, hearkening back to its historic definition from 1999 to maximize participation in recognition of the Act's security objectives.[24] A key purpose of the Secure Networks Act is to help small and rural providers, some of whom may be trying to

---

[22] Secure Networks Act § 8(a)(1).

[23] *Id.* at § 9(1); Telecommunications Act of 1996 § 706(c)(1), Pub. L. No. 104-104, 110 Stat. 56, 153.

[24] FCC, Declaratory Ruling and Second Further Notice of Proposed Rulemaking, *Protecting Against National Security Threats to the Communications Supply Chain Through FCC Program*, WC Docket No. 18-89, FCC 20-99, at ¶ 27 (rel. July 17, 2020) ("FCC Declaratory Ruling and Second FNPRM").

upgrade legacy networks or even offering broadband for the first time, and NTIA should ensure that those providers can be included. Indeed, any established telephone company seeking to *become* a provider of advanced services for the first time should be eligible to receive at least some basic information, lest the statutory purpose be defeated.

Regarding suppliers, the issue is somewhat more complex. As noted above, participation in the program is extended to "trusted suppliers of communications equipment or services." The term "communications equipment or service" is further defined by the Secure Networks Act to mean "any equipment or service that is *essential* to the provision of advanced communications service."[25] If this definition is applied literally in considering whether a particular supplier can participate in the Section 8 information sharing program, this may be a difficult calculation to make.

First, it may be difficult to categorize any particular type of equipment or service as "essential" for a particular network. Providers have many options, including both wired and wireless technologies, and some traditional elements of a network such as a base station are increasingly being disaggregated or replaced by service-based alternatives. Second, equipment can be used in different ways. The same piece of equipment could be used to provide both basic wireline telephone as well as broadband service of varying speeds. It might be used to provide both Wi-Fi and commercial mobile radio services like 4G. It might be used in an edge network for customer access, or deeper in a core network where its relevance to particular customers may be harder to discern.

The FCC is currently grappling with defining the same term, and has offered the following explanation for its proposed approach:

[25] Secure Networks Act § 9(4) (emphasis added).

> We propose to include within this definition of "communications equipment or service[s]" all equipment or services used in fixed and mobile broadband networks, provided they include or use electronic components. We believe that all equipment or services that include or use electronic components can be reasonably considered essential to broadband networks. Moreover, the presence of electronic components provides a bright-line rule that will ease regulatory compliance and administrability.[26]

Since the purpose of the Act is to promote security, participation by suppliers in the information program should be construed reasonably broadly. The proposed FCC language above suggests a broad definition, that, if applied here, would include most or all suppliers. This is philosophically the right approach, and drawing hard lines may be unnecessary for purposes of Section 8 of the Act given that NTIA is establishing an information sharing program.[27]

To the extent that any line-drawing is required about whether a particular supplier's products or services are "essential" to advanced communications service, thus allowing it participate in the Section 8 program, a more functional test may be appropriate. For example, if there were any doubt about a particular supplier, NTIA could simply require it to demonstrate that it currently sells or has concrete plans to sell its products and services to a "trusted provider of advanced communications service."

[26] FCC Declaratory Ruling and Second FNPRM, *supra* n. 24, at ¶ 26.

[27] The actual proposed FCC definition still uses the word "essential." *See id.* at Appendix A (proposing 47 C.F.R. § 1.40001(c)). This might be somewhat circular in light of the assertion above that anything using electronic components can "reasonably be considered essential." In addition, the FCC's proposed focus on products that "include or use electronic components" seems too broad in light of Section 2(b)(2) of the Secure Networks Act, which focuses on equipment that is "capable of routing or redirecting user data traffic or permitting visibility into any user data or packets that such equipment or service transmits or otherwise handles." But for purposes of Section 8, this does not matter.

III. THE INFORMATION SHARING PROGRAM SHOULD INCLUDE BOTH "PUSH" AND "PULL" ELEMENTS.

The Secure Networks Act requires NTIA to "conduct regular briefings and other events to share information" with participants and to "engage" with participants.[28] To implement these requirements most effectively, the information sharing program should include both "push" and "pull" elements. On the "push" side, NTIA should regularly provide participants with opportunities to receive briefings and other information, as contemplated by the law. NTIA should also regularly "engage" at carrier and industry forums and conferences to publicize the agency's risk information sharing program for small and rural providers and businesses. NTIA should also consider collaborating with the FCC to bring greater awareness of its program: for example, the FCC could include non-mandatory mentions of the program on its website, and even on certain forms or applications that small businesses may have occasion to review as part of their regular dealings with the agency. The FCC might also consider inviting NTIA to brief stakeholders on the program during relevant advisory committee meetings such as the Broadband Deployment Advisory Committee (BDAC) or the Communications Security, Reliability, and Interoperability Council (CSRIC) meetings.

On the "pull" side, NTIA should permit eligible providers and suppliers to proactively and confidentially ask for risk and vulnerability information about specific equipment, software, and services. Particularly in the case of small providers and suppliers, systemic equipment upgrades or significant supply chain changes may happen irregularly, often at intervals of a decade or more. Providers doing major upgrades – such as from 4G or earlier technologies to 5G – should be able to receive the information at the right moment to inform their procurement

[28] Secure Networks Act §§ 8(a)(2)(A), (B).

decisions. The same principle would apply to a *supplier* considering changing its manufacturing to a different country, or sourcing key components like chips from a different upstream supplier. Risk information needs to be available easily and quickly at the moment purchasing decisions are being made.

To facilitate this, NTIA should establish a single point of contact at the agency to field such queries – perhaps even a hotline of sorts – and the answers given should be brief and provided quickly. However, to the greatest extent possible, NTIA should ensure that such requests for information remain confidential. Without such protection, a company's consideration of particular products and services, or the advice given by NTIA and taken (or not taken) by the requestor, could create liability that might dissuade companies from asking the agency for help or have anticompetitive implications.

CONCLUSION

CompTIA appreciates NTIA's work toward establishing the information sharing program required by Section 8 of the Secure Networks Act. Information sharing offers a meaningful and practical path toward improving supply chain security issues for communications networks, and CompTIA's members look forward to engaging with NTIA on these issues as the program is launched.

Sincerely,

/s/ Dileep Srihari

Dileep Srihari
Vice President and Senior Policy Counsel

Savannah Schaefer
Senior Director, Public Advocacy

COMPUTING TECHNOLOGY INDUSTRY ASSOCIATION (CompTIA)
322 4th Street NE
Washington, DC 20002

July 28, 2020