October 31, 2017

Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

To Whom It May Concern:

On behalf of the Communications Sector Coordinating Council ("CSCC") please find below responses to the questions posed by the Government Accountability Office ("GAO") in its new inquiry U.S. Government Accountability Office engagement on Cybersecurity Framework Adoption – code 101948. The GAO is interested in learning about private sector use of the *NIST Framework* for *Improving Critical Infrastructure Cybersecurity* ("the *Framework*").

The Communications Sector Coordinating Council (CSCC), with its government partners, works to protect the Nation's communications critical infrastructure and key resources from harm and to ensure that the Nation's communications networks and systems are available, secure, resilient, and rapidly restored after a natural or manmade disaster. In carrying out this mission, the CSCC's goals are to:

- Protect and enhance the overall physical and logical/cyber health of communications;
- Rapidly reconstitute critical communications services in the event of disruption and mitigate cascading effects;
- Improve the sector's NS/EP posture with Federal, State, Local, Tribal, Territorial, and private sector entities to reduce risk.

The Communications Sector is encouraged by the success of the *Cybersecurity Framework* in raising awareness and promoting risk management instead of a checklist approach to cybersecurity. Given its flexibility and utility, as well as the extensive work that has been put into the *Cybersecurity Framework*, it is imperative that the government maintain and promote it, instead of moving in a more regulatory or prescriptive direction. The CSCC is pleased to explain to GAO how the Communications Sector has been actively engaged in promoting the *Cybersecurity Framework.*

GAO QUESTION #1: WHAT ACTIVITIES, IF ANY, HAS YOUR SECTOR PARTICIPATED IN TO PROMOTE THE USE OF THE CYBERSECURITY FRAMEWORK AMONGST MEMBERS OF THE COMMUNICATIONS SECTOR?

The answer to this question is multifold and extensive. The Communications Sector has long been engaged in cyber risk management, helped shape the *Cybersecurity Framework,* uses the Framework enthusiastically, , and is collaborating with NIST on its next iteration. Sector

companies also do many things separate from the Cybersecurity Framework that are complementary and consistent with its core risk management message.

***First,* the Communications Sector has been engaged in cyber risk management for decades, and drew on that experience to help create the Cybersecurity Framework.** The risk management principles in the Framework are not new to the Communications Sector. Many companies across the sector had mature cybersecurity policies and programs already. In many cases, the Framework reflects and complements those established postures. Specifically, many companies, particularly the large operators, have long embraced and implemented risk management principles, and have used industry best practices and international standards—many of which appear as Informative References in the Framework.

As Verizon described its approach prior to the *Cybersecurity Framework*, its "policies and practices in the areas of network security, information security, personnel security, and physical security are informed by a wide range of industry standards. As part of its process to define its security controls, Verizon examines numerous externally-developed standards, including [NIST Special Publications 800 series, ISO 27001/27002, GAISP, NRIC and CSRIC Best Practices, SAS 70, PCI Data Security Standard, FISMA requirements and practices, Australian Top 5 controls, SANS Tip 20 controls, NERC CIP-002 to CIP-009, COBIT, QUEST Forums, DHS Cyber Security Framework and Technical Metrics, and various other industry standards.] Notably, Verizon does not follow each and every practice contained in the above-referenced publications. Rather, Verizon creates its own set of practices to address the specific security needs of Verizon's network infrastructure by tailoring the standards from the various sources."[1]

Communications Sector companies include cyber risk in their broader risk management. They invest billions of dollars and deploy multiple layers of security from core networks to device design and application integrity. They also invest in cybersecurity research and development, and are developing the latest technologies, strategies, and features with security in mind—such as software-defined networks, new authentication methods, and integrated hardware and software products.

Representatives of the Communication Sector participated extensively in creating the Framework. This included the 2013 NIST workshops and all drafting phases of the Framework. Individual members also engaged in the public comment process. Members found the process to be collaborative and effective.

Second, the Communications Sector has promoted and used the *Cybersecurity Framework* in CSRIC, in outreach to small businesses, and in numerous public engagements.

1. FCC CSRIC Efforts Have Utilized and Promoted the Framework

Following the release of Version 1.0 of the *Framework*, the Communications Sector launched a robust effort to "provid[e] implementation guidance to help communications providers use and adapt the voluntary [*Framework*]."[2] This effort, in the Federal Communications Commission's

[1] Verizon Comments to NIST (Apr. 8, 2013), https://www.nist.gov/file/369351.

[2] *See* CSRIC IV, Working Group 4, *Cybersecurity Risk Management and Best Practices: Final Report* (2015) ("CSRIC IV Final Report").

("FCC") Communications Security, Reliability, and Interoperability Council ("CSRIC") IV Working Group 4, mapped the *Framework* across the five Communication Sector industry segments: broadcast, cable, satellite, wireless, and wireline. It involved over 100 experts representing the industry, state and federal government stakeholders, equipment manufacturers, and cybersecurity solutions providers, among others. It also specifically addressed small and medium companies who face unique challenges.

CSRIC IV Working Group 4's final report, *Cybersecurity Risk Management and Best Practices* ("*CSRIC IV Report*"), applies the *Framework* to each industry segment.[3] Among other things, the *CSRIC IV Report* identifies communications sector standards that help implement the *Framework.* The goal was two-fold: in addition to providing implementation guidance, CSRIC wanted to "give the [FCC] and the public assurance that communications providers are taking the necessary measures to manage cybersecurity risks across the enterprise."[4] This effort has become the baseline for Communications Sector cyber risk management using the *Framework.*

Other CSRIC efforts promote the *Framework* and risk management.

- CSRIC IV Working Group 5's report, *Remediation of Server-Based DDoS Attacks*, relies heavily on the *Framework*.[5]
- CSRIC V Working Group 5's report on *Cybersecurity Information Sharing* encourages cybersecurity information sharing "across the communications sector to all stakeholders necessary to successfully execute the 'protect, detect, respond, and recover' functions of the NIST *Cybersecurity Framework*."[6]
- CSRIC V Working Group 6 used the *Framework* to address Security-by-Design.[7]

2. The Communications Sector Engages in Outreach to Small- and Medium Sized Companies and Others in the Ecosystem

CSCC members promote the *Framework* throughout the Communications Sector, including to small- and medium-sized companies. As T-Mobile highlighted in a blog post intended to promote cybersecurity best practices, "[s]mall businesses don't get a pass when it comes to cybersecurity threats. Size does not matter to hackers, scammers and other online criminals wanting to make a quick buck at your company's expense."[8] Similarly, AT&T produces resources for businesses—large and small—to manage cybersecurity, such as *The CEO's Guide to Data Security*.[9]

---

[3] *Id.*

[4] *Id.*

[5] CSRIC IV, Working Group 5, *Remediation of Server-Based DDoS Attacks: Final Report* (2014) ("The Working Group conducted a gap analysis using The Six Phases of DDoS Attack Preparation and Response in parallel with the NIST Cybersecurity Framework.").

[6] CSRIC V, Working Group 5, *Cyber Security Information Sharing: Final Report* (2017) ("*CSRIC V, WG 5 Report*").

[7] CSRIC V, Working Group 6, *Secure Hardware and Software: Security-By-Design: Final Report* (2016).

[8] *Why Cybersecurity Should Be Your Top Priority in 2017*, T-Mobile Business Hub, https://businesshub.t-mobile.com/articles/why-cyber-security-should-be-your-top-priority-2017.

[9] https://www.business.att.com/cybersecurity/docs/vol5-datasecurity.pdf.

Representatives of the Communications Sector have created the Multi-Association Framework Development Initiative (MAFDI). "The initiative, co-chaired by the US Telecom Association Senior Vice President and the Information Technology Industry Council Vice President, includes 32 US-based trade associations. The MAFDI group's four key goals are: (1) to include engaging multiple stakeholders in coordinating views of the use and evolution of the NIST framework and any external factors that could affect the viability of the model; (2) to share information across sectors on specific NIST framework activities and experiences with regulators and other stakeholders; (3) to work to promote the framework as an international model; and (4) to bring key influencers from government to hear their perspectives, learn of new initiatives and share industry interests and concerns."[10]

3. The Communications Sector Promotes the *Framework* in Public Engagements

Communications Sector members and associations participate in public events to promote the *Framework* and cyber risk management. For example, CTIA convened a *Cybersecurity Summit* in May 2017 in Washington, DC, to address the current cyber threat landscape, the innovative technologies that are addressing these challenges today, and what actions our country's policymakers should take as we move toward the more connected 5G networks of tomorrow.

NTCA–The Rural Broadband Association has committed significant resources to ensuring its members are informed about the NIST Cybersecurity Framework and its underlying risk management approach to cybersecurity. The association provides continuing education for small, rural communications service providers, and related vendors and consultants. In 2016 alone, more than 2,000 attendees participated in a dozen NTCA-led events around the country. For instance, NTCA's Cybersecurity Summit in October 2016 featured the latest trends and threats in the cybersecurity space, industry best practices to address to those threats, and a summary of recent government action taken to address cybersecurity liabilities. And in 2017, NTCA's Cybersecurity Summit and related online and on-site cybersecurity educational events drew more than 1,500 attendees. NTCA also convened a member cybersecurity working group to discuss technical, operational and policy considerations related to evolving cyber threats.

In addition, in October 2016, NTCA released the NTCA Cybersecurity Bundle, a comprehensive guide that includes three key components: a risk-management primer, an operational template, and industry resources. These components are designed to work together to help telco executives, board officers, and operational staff develop a risk-management approach to cybersecurity, based upon the NIST Cybersecurity Framework and the sector-specific guidance as developed by the FCC's CSRIC IV WG4 for Small and Mid-sized business Group.

Several statewide telecom associations also have convened regional events to educate small ISPs about cybersecurity risk management and how small telecommunications companies can use the NIST Cybersecurity Framework. For instance, SDN Communications, a regional fiber network provider, led the NIST Cybersecurity Framework Training event in May 2016 in Sioux Falls, S.D., in partnership with the South Dakota Telecommunications Association and Dakota State

[10] *CSRIC V, WG 5 Report.*

University (DSU). The Iowa Communications Alliance also offered regional cybersecurity training events in April 2016 and April 2017.

Furthermore, in January 2017, the American Cable Association (ACA) held an educational webinar for its members on "Cybersecurity and Supply Chain Risk Management for Small ISPs." During the webinar, representatives from the federal government, including William "Bill" Evanina, National Counterintelligence Executive and Director of the National Counterintelligence and Security Center Office of the Director of National Intelligence (ODNI), Rear Admiral (Ret.) David G. Simpson, who was then Chief of the FCC's Public Safety and Homeland Security Bureau, and staff members from the FBI, NIST, and ODNI, discussed the threats facing small and mid-size businesses, as well as steps they can take to identify, prevent, and mitigate them. ACA plans to host similar events in the future, focusing on practical steps that members can take to improve their cybersecurity posture.

On March 23, 2017, the National Association of Broadcasters (NAB) assembled a panel of experts for a webcast, titled "Cybersecurity: The Next Steps," to provide its members with a framework for preparing your broadcast operation in the event of a cyberattack. Progressing from the NIST Framework and recommendations by the Communications Security, Resiliency and Interoperability Council (CSRIC), the panel focused on how to enhance your existing disaster recovery and continuity of operation plans in anticipation of a cyberattack. Speakers included Mike Kelley (The E.W. Scripps Company) and Mike Funk (Quincy Media). NAB will announce other similar educational opportunities for the members in the coming months.

NAB, along with the World Broadcasting Unions – International Media Connectivity Group, also co-sponsored a two-day event on May 31 and June 1 that covered a number of topics related to cybersecurity, including common cybersecurity issues faced by media and content companies. The group also released two White Papers for broadcasters: "Essential Guide to Broadcast Cybersecurity" and "35 Critical Cyber Security Activities." Both set forth recommendations and tools to help broadcasters secure and maintain operations in the face of increasing digital security threats. Reports highlight the key resources that broadcasters can rely upon in assessing, protecting and containing cyber intrusions. Both build off the NIST Cybersecurity Framework and the application of that Framework to broadcasting in the context of the FCC CSRIC IV Working Group 4 report on cybersecurity.

NCTA – The Internet & Television Association (NCTA) and its members are engaged in a wide range of public activities and collaboration on cybersecurity, participate in public events to promote the *Framework* and cyber risk management. Cable ISPs play a leading role in organizations engaged in cutting-edge cybersecurity work, including developing best practices and technical papers under the auspices of the Messaging, Malware and Mobile Anti-Abuse Working Group (MAAWG), the Broadband Internet Technical Advisory Group (BITAG), and the Internet Engineering Task Force (IETF). Public engagement promoting the Framework and its principles also includes:

- The Comcast Center of Excellence for Security Innovation at the University of Connecticut (CSI) has hosted CyberSeed in 2014, 2015, 2016, and 2017. CyberSEED brings together top information security professionals and business leaders to discuss emerging cybersecurity trends and formulate the best strategies for tackling current and future threats.

- In April 2017, CableLabs hosted the Inform[ED] IoT Security conference. The conference brought together business leaders, key technologists, security experts and policymakers to discuss a range of issues with connected devices, including hacking, protecting ISP networks, and standards. The discussions also addressed how to apply the Framework to IoT security.[11]
- At the 2015 Society of Cable Telecommunications Engineers (SCTE) Cable-Tech EXPO, SCTE and CableLabs co-hosted the Cybersecurity Symposium. The symposium brought together leaders from the cable industry to discuss how the Framework is being used by the cable industry to secure their networks. During NCTA's Spring Technical Forum, held in conjunction with the cable industry's 2015 INTX show, cable companies presented a paper on various ways that the cable industry secures its infrastructure and showed how this mapped back to the Framework.

Additional sector activities promoting the Framework and its principles include:

- November 2014 (Austin, TX): **Dell World 2014**: NIST's Dr. Ron Ross and DELL CSO John McClurg discussing NIST and the New Cybersecurity Framework.
- March 2015 (Arlington, VA): **Department of Homeland Security ISAC-ISAO Summit** featured USTelecom speaking about the commitment that the telecom sector will continue to make on the NIST Framework and the new Information Sharing effort going forward.
- March 2015 (Washington, DC): **National Cybersecurity Policy Forum: Report Showcases Industry Use of NIST Framework**
- June 2015 (Williamsburg, VA): **Mid-Atlantic Conference of Regulatory Utilities Commissioners (MACRUC) 20th Annual Education Conference:** USTelecom addressed the impact of the Communications Security, Reliability and Interoperability Council IV, Working Group 4 report on cybersecurity risk management and best practices on all segments of the telecommunications industry (broadcast, cable, satellite, wireless and wireline), and discussed ways to implement the National Institute of Standards and Technology Cybersecurity Framework for all size companies.
- July 2015 (New York, NY): **NARUC Summer Committee Meetings**: USTelecom provided an overview of the "Cybersecurity Risk Management Guide for Voluntary Use" of the NIST Cybersecurity Framework and discussed strategies for rationalizing state inquiries.
- September 2015 (Hamilton, NJ): **Cyber Community Voluntary Program 2015 Regional Event: Managing Cyber Risk - Resources for State and Local Governments and Small and Midsize Businesses**: USTelecom talked about the efforts of the communications sector to develop an adaptation of the NIST Cybersecurity

[11] *A Vision for Secure IoT*, CableLabs (Summer 2017), http://www.cablelabs.com/vision-secure-iot/. This paper details the technical goals of an industry-led approach to IoT device security, as well as the governance goals of the development organization. The paper recommends that such an undertaking address such key issues as: (i) device identity; (ii) authentication, authorization, and accountability (onboarding); (iii) confidentiality; (iv) integrity; (v) availability; (vi) lifecycle management; and (vii) future (upgradable) security.

Framework to the broadcast, cable, satellite, wireless and wireline industries. Also discussed efforts by member companies to adapt the framework to their unique enterprise risk management structure.

- May 2016 (Webinar): **C³ Voluntary Program Webinar Series:** USTelecom presented as part of a webinar series on the use of the NIST Framework. The first webinar provided an overview of the C³ Voluntary Program and other program activities, while later webinars featured topics such as incorporating threat information into Framework use and communicating about cybersecurity with the C-suite.
- October 2016 (New York, NY): The **AT&T Cybersecurity Conference** focused on cloud security, mobile security, network security, and the threat landscape.
- December 2016 (New York, NY): **Service Provider & Enterprise Security Strategies** featured a CTIA representative as a speaker.
- February 2017 (San Francisco, CA): The **RSA Conference** featured several Communications Sector members, including Cisco, HP, Intel, and Verizon.
- March 2017 (Blacksburg, VA): The **Virginia Tech CyberLeaders Seminar Series** featured a CTIA representative as a speaker. June 2017 **CREATe's** Cybersecurity Advisory Council released report: **Broadening Adoption of the NIST Cybersecurity Framework:** ***Learnings from the CREATe Cybersecurity Advisory Council about the Key Ways to Help Companies Operationalize Leading Practices for Cybersecurity*****.** The Communications Sector has a representative member from AT&T on the Cybersecurity Advisory Council, which was created to share best practices and lessons learned from using the Framework across a range of industries. The purpose of the report was to "help companies to better leverage guidance from the Framework and operationalize the results."
- July 2017 (Washington, DC): **USTelecom Cybersecurity Policy Forum 2017**. https://www.ustelecom.org/events-education/executive-education/ustelecom-cybersecurity-policy-forum-2017 (featuring government and Communications Sector leaders)
- August 2017 (Boston, MA): The **National Conference of State Legislatures Summit** addressed cyber issues with a CTIA representative as a panelist.
- September 2017 (San Francisco, CA): The **GSMA Mobile World Congress Americas in partnership with CTIA** covered cybersecurity, for example with a panel dedicated to IoT security,[12] and awards given to cybersecurity/wireless industry startups.[13]
- October 2017 (Washington DC): The **Fifth Annual Internet of Things Global Summit** focused on cyber, with a panel discussion featuring Communications Sector members, including CTIA.

Third, the Communications Sector is working actively with NIST on the *Cybersecurity Framework Version 1.1*.

---

[12] *See Cybersecurity: From the Device to all of IoT*, https://www.mwcamericas.com/start-here/agenda/cybersecurity-from-the-device-to-all-of-iot/.

[13] *See* https://www.mwcamericas.com/session/4yfn-americas-awards-finale-i-cybersecurity-wireless-industry-startups/.

Following the release of the *Cybersecurity Framework* Version 1.0, NIST continued collaborating with stakeholders. The Communications Sector actively engaged. In 2014, NIST inquired about experience with the *Framework*, and companies filed detailed comments.[14]

In late 2015, NIST sought more comment on the *Framework*. The Sector filed comments explaining that the Communications Sector is using the *Framework* in multiple efforts, including in the FCC's CSRIC.[15] AT&T described the *Framework* as "the best vehicle to improve the cybersecurity posture of critical infrastructure and other entities," and highlighted that the *Framework* is built on the concept of risk management.[16] iconectiv explained that it was "applying the [*Framework*] as part of our risk management program."[17]

The Sector has been active as NIST considers updates to the *Framework* with Version 1.1. Companies and associations filed comments in response to NIST's request for feedback on its January 2017 draft Version 1.1.[18] Companies and associations in the Communications Sector were integral in the May 2017 NIST Workshop regarding the *Framework* Version 1.1. Specifically, the Communication Sector hosted a panel, *The Sector Customization Process – The Communications Sector*, which highlighted that "within the Communications Sector, a number of organizations have developed their own methods to measure the effectiveness of NIST Cybersecurity Framework adoption."[19] The panel featured USTelecom, AT&T, CenturyLink, CTIA, NCTA, and NTCA.

The Communications Sector submitted to NIST further feedback, including a redline of the proposed new section on measurements and metrics, urging NIST to promote a voluntary, self-assessment approach, in line with risk management. CSCC participants, and trade associations, have had an open dialogue with NIST staff regarding the *Cybersecurity Framework* for years, and look forward to continued collaboration.

Finally, the Communications Sector uses and promotes many of the broader risk management principles that are embodied in the *Cybersecurity Framework*. The Communications Sector promotes the core tenets of the *Cybersecurity Framework*. For example, collaboration is integral to security.[20] Three examples illustrate this:

1. **The Sector Aggressively Detects Malicious Activity and Respond to Threats**.

---

[14] CTIA Comments to NIST (Oct. 10, 2014), *available at* https://www.nist.gov/file/346541.
[15] CTIA Comments to NIST (Feb. 23, 2016), https://www.nist.gov/file/351781.
[16] AT&T Comments to NIST (Feb. 23, 2016), *available at https://www.nist.gov/sites/default/files/documents/2017/02/14/20160223_att.pdf*.
[17] iconectiv Comments to NIST (Feb. 8, 2016), *available at* https://www.nist.gov/sites/default/files/documents/2017/02/13/20160208_iconectiv.pdf.
[18] *See,e.g.*, CTIA Comments to NIST (Apr. 10, 2017), *available at* https://www.nist.gov/file/362641; USTelecom Comments to NIST (Apr. 10, 2017) *available at* https://www.ustelecom.org/sites/default/files/documents/USTelecom-Comments-2017-04-07-FINAL_0.pdf ; Comments of NCTA (Apr. 10, 2017) available at https://www.nist.gov/sites/default/files/documents/2017/04/19/2017-04-10_-_ncta.pdf
[19] NIST, *What We Heard* (May 2017 Workshop), *available at* https://www.nist.gov/file/366391.
[20] NIST, *Background: Framework for Improving Critical Infrastructure Cybersecurity* (Aug. 20, 2016), http://www.nist.gov/cyberframework.

The Communications Sector is constantly responding to threats. AT&T's security experts see more than 30 billion vulnerability scans and 400 million spam messages cross its network every day; and 5 billion vulnerability scans and 200,000 malware events targeted at its network every day.[21] There has been a 3,198% increase in vulnerability scans of IoT devices over the past 3 years.[22] Google checks more than 6 billion apps, and it scans 400 million devices each day.[23]

These efforts depend on industry evolving, and responding to changes. For example, the ecosystem is constantly refining how to communicate vulnerability information among Operating System providers, manufacturers, and carriers.[24] Additionally, the industry is focused on the next wave of technology, including a transition to all-digital, 5G technology and the IoT. In this transition period, the industry is enhancing security through including improved encryption, distributed and secure architecture, and decentralized and adaptive security.

2. Consumer Education is Key and Led by the Communications Sector.

CTIA and industry are dedicated to providing consumers and end users with information and tools to help protect data, devices, and networks. Industry is engaged in significant public-private efforts to educate consumers and enterprise end users, including White Papers,[25] a variety of online content for consumers to access regarding cybersecurity,[26] and CTIA's consumer tips.[27] For example, CTIA and the wireless industry have long encouraged consumers to be vigilant in safeguarding their mobile devices through initiatives such as the Smartphone Anti-Theft Voluntary Commitment launched in 2014, under which industry participants agreed to provide remote wipe capabilities on new smartphones among other security measures. The Stolen Phone Checker website launched in May 2017, providing consumers the ability to determine if a used or refurbished smartphone has been reported as lost or stolen.

As threats evolve, the wireless industry will continue to provide consumers with the tools and knowledge to protect themselves. Additionally, CTIA engages in research to assess consumers' use of security features, and this research shows our efforts are effective.[28] In October 2017, CTIA announced new survey results showing that America's wireless consumers continue to

---

[21] Chris Boyer, *How the Public Safety Bureau Paper Gets Cybersecurity* Wrong, AT&T Public Policy Blog (Jan. 25, 2017), https://www.attpublicpolicy.com/cybersecurity/how-the-public-safety-bureaupaper-gets-cybersecurity-wrong/.

[22] *Id.*

[23] Android Security 2015 Annual Report (Apr. 2016), https://security.googleblog.com/2016/04/android-security-2015-annual-report.html.

[24] *See Android, Android Security Bulletin—August 2016* (Aug. 1, 2016), https://source.android.com/security/bulletin/2016-08-01.html; *CVE Details, Google Android: List of Security Vulnerabilities*, https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html.

[25] *See, e.g., http://files.ctia.org/pdf/CTIA_IndustryMegatrends_Consumers.pdf*

[26] *See, e.g.*, https://www.ctia.org/industry-data/blog-details/blog-posts/ncsa-stop-think-connect.

[27] *See, e.g.*, How to Stop Robocalls, https://www.ctia.org/consumer-tips/robocalls; How to Deter Smartphone Thefts and Protect Your Data, https://www.ctia.org/consumer-tips/how-to-deter-smartphone-thefts-and-protect-your-data.

[28] *See, e.g.*, Protecting America's Wireless Networks; *Smartphone users are becoming more aware of security features*, Business Insider (Aug.3, 2016, 8:30 PM), http://static3.businessinsider.com/smartphone-users-are-becoming-more-aware-of-security-features-2016-8.

adopt more advanced security measures for their mobile devices amid ongoing consumer protection and education efforts. The survey, conducted by Harris Poll found that:

- 77 percent of Americans use PINs/passwords on their smartphones, a 54 percent increase in the last five years.
- Nearly 50 percent of Americans have an anti-virus program installed on their smartphone, a 58 percent increase in the last five years.
- Nearly 60 percent of Americans report having the ability to remotely locate, lock and erase software on their smartphones, a 43 percent increase in the last five years.

3. Information Sharing Occurs Within the Sector and with Government.

The CSCC itself is a prime example of the sort of information sharing that has helped the Communications Sector address cybersecurity risk, and which promotes the sort of collaboration that is called for in the *Cybersecurity Framework*. Our sector and its members engage with several government agencies and key players regarding cybersecurity. Public-private partnerships, driven by industry, abound.

Department of Homeland Security

- The Communications Sector has partnered with DHS in venues like the National Cybersecurity and Communications Integration Center ("NCCIC"), for decades. Several large carriers are embedded with the NCCIC, facilitating real-time detection, response and information-sharing, all key functions of the *Framework*.
- Industry is engaged with DHS through the Communications Sector Coordinating Council ("CSCC"), which facilitates coordination on a range of sector-specific strategies and activities, and which releases important White Papers.[29]
- The COMM-ISAC is the only public-private Information Sharing and Analysis Center and DHS' National Coordinating Center (NCC) provides the 24/7 watch desk functions for this highly robust capability. . The communications sector is well-represented on the COMM-ISAC, with participants including the major associations and the large operators, among other stakeholders.
- Communications Sector representatives serve as members and leaders of the National Security Telecommunications Advisory Committee ("NSTAC"), appointed by the President to make recommendations about security.[30] Members of the NSTAC include many Communications Sector leaders.[31]
- The Communications Sector is actively working on enhancing automated information sharing. Communications sector companies partner with DHS to share cyber threat

---

[29] *See, e.g.*, CSCC, Industry Technical White Paper (July 17, 2017), *available at* https://docs.wixstatic.com/ugd/0a1552_18ae07afc1b04aa1bd13258087a9c77b.pdf *("Botnet White Paper").*

[30] https://www.dhs.gov/nstac-members.

[31] *Id.*

indicators through Automated Indicator Sharing ("AIS") and have participated in a *Cyber Threat Information Sharing Pilot.* CTIA recently completed an important information sharing trial, inspired by the Cybersecurity Information Sharing Act of 2015 and CSRIC's Information Sharing Report. The successful pilot effort involved CTIA members sharing certain cyber information—including AIS—to detect and mitigate Telephone Denial of Service ("TDoS") attacks and robocall activities.

- Further, many Communication Sector members are participants in DHS information sharing programs including the National Security Information Exchange (NSIE), and Cyber Information Sharing & Collaboration Program (CISCP).

Federal Communications Commission. CSCC participants, through the CSRIC and other venues, work with the FCC on voluntary cyber efforts and the identification of best practices and solutions to common challenges. This effort is extensive and ongoing.

NIST. Communications Sector companies have a productive relationship with NIST, including its NCCoE. Companies and their associations regularly provide input to NIST regarding its burgeoning body of work on cybersecurity. Additionally, NIST's Information Security and Privacy Advisory Boards ("ISPAB")—the body charged with advising the Secretary of Homeland Security and the director of OMB on information security and privacy issues pertaining to federal government information systems, and which reviews proposed NIST standards and guidelines—is chaired by a representative of AT&T.[32] ISPAB had a role in the development of the *Cybersecurity Framework*.[33]

NTIA. CSCC participants have engaged in NTIA stakeholder efforts, including efforts to combat botnets,[34] to explore options for cybersecurity vulnerability disclosures,[35] and to better secure the IoT.[36] Sector participants consistently urge NTIA to rely on the *Framework* as a key approach to managing cyber risk

The associations all have focused working groups on cybersecurity that share best practices and uses of the Framework.

- **CTIA leads the wireless sector's efforts.** Through CTIA's Cybersecurity Working Group ("CSWG"), CTIA members representing the entire mobile ecosystem engage in research and dialogue with private sector and government entities including NIST, the Department of Homeland Security ("DHS"), FCC, and several others. The CSWG, which convenes bi-weekly calls and quarterly face to face meetings, shares active threat information and promotes collaboration by technical and policy personnel from companies and government. It produces White Papers on topics such as consumer cyber

---

[32] https://www.nist.gov/news-events/news/2016/04/nists-information-security-and-privacy-advisory-board-names-new-chair.

[33] *See, e,g.,* https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/correspondence/ispab_ltr_on_cybersec-framework_jan2014.pdf.

[34] *See* https://www.ntia.doc.gov/federal-register-notice/2017/rfc-promoting-stakeholder-action-against-botnets-and-other-automated-threats.

[35] *See* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities.

[36] *See* https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.

education,[37] information sharing,[38] cybersecurity of mobile devices and the Internet of Things,[39] and cybersecurity in the new 5G network.[40] The CSWG conducts and supports academic research that yield tools for device management, anti-malware, browsing protection, app reputation checking, call/short message service blocking and scanning, and firewalls. Recently, CSWG's research is focusing on IoT threats, 5G vulnerabilities, and robocalling.

- **USTelecom plays a leading role for ISPs and wireline companies.** It organizes advocacy with members, other trade associations and government partnership councils and committees. It regularly convenes policy discussions with top officials in the White House, executive and legislative arena and critical infrastructure industries through the National Cybersecurity Policy Forum series https://www.ustelecom.org/events-education/national-cybersecurity-policy-forum.

- **NCTA, the Internet & Television Association, leads the cable ISP sector's efforts**. NCTA's Cybersecurity Working Group ("NCTA-CSWG"), comprised of cybersecurity and technology experts from member companies, meets regularly to share information on the latest threats, cyber defense tools, and best practices. NCTA-CSWG's discussions about different strategies and practices companies may employ in managing cyber risks benefit from the Framework's shared language and informative references. In July 2017, NCTA and members of NCTA-CSWG were the principal authors of a communications sector technical white paper on mitigating botnets and automated attacks from the perspective of ISPs. The NCTA-CSWG convenes bi-weekly calls and twice a year face-to-face meetings.

- **CCA helps competitive wireless carriers and stakeholders address cyber, recently joining the Comm-ISAC and addressing cyber.**

Domestic and International Standards Bodies. Industry works with domestic and international standards bodies—like 3rd Generation Partnership Project ("3GPP"), Alliance for Telecommunications Industry Solutions ("ATIS"), European Telecommunications Standards Institute ("ETSI"), Institute of Electrical and Electronics Engineers, Inc. ("IEEE"), Internet Engineering Task Force ("IETF"), oneM2M Partners ("oneM2M"), Open Connectivity Foundation ("OCF"), Society of Cable & Telecommunications Engineers ("SCTE"), and GSM Association ("GSMA")—to develop network security standards that are comprehensive and effective. In addition to standards bodies, communications sector companies also actively engage in multisakeholder working groups such as the Messaging, Malware and Mobile Anti-

---

[37] *See* CTIA, *Today's Mobile Cybersecurity: Industry Megatrends & Consumers, available at* http://files.ctia.org/pdf/CTIA_IndustryMegatrends_Consumers.pdf.
[38] *See* CTIA, *Today's Mobile Cybersecurity: Information Sharing, available at* https://www.ctia.org/docs/default-source/default-document-library/ctia_informationsharing.pdf.
[39] *See* CTIA, *Mobile Cybersecurity and the Internet of Things: Empowering M2M Communication, available at* http://www.ctia.org/docs/default-source/default-document-library/ctia-iot-white-paper.pdf.
[40] *See* CTIA, *Protecting America's Wireless Networks, available at* https://www.ctia.org/docs/default-source/default-document-library/protecting-americas-wireless-networks.pdf.

Abuse Working Group (M3AAWG). Communications Sector companies participate in these groups in leadership roles.

International Efforts to Promote the Framework and Framework Principles. Communications Sector companies and representatives work to promote the Framework by name, as well as its underlying principles internationally at conferences, industry events, and during informal and formal government-industry engagement. Companies also regularly partake in the public comment process on legislative, regulatory and policy proposals from foreign governments. Whether under company name or via coalition submission, sector members frequently utilize the public comment process to promote the NIST Framework, and the principles embodied therein as a model approach to cybersecurity worldwide. Moreover, companies in the Communications Sector regularly participate in cybersecurity capacity building efforts geared at developing nations. Such venues also provide the sector with opportunity to promote the NIST Framework.

GAO QUESTION #2: WHAT ACTIVITIES, IF ANY, ARE PLANNED TO PROMOTE THE USE OF THE *CYBERSECURITY FRAMEWORK*?

As noted above, numerous activities occur to promote risk management and the Cybersecurity Framework. The Communications Sector will continue to promote cybersecurity risk management. Notably, however, NIST is currently updating the *Cybersecurity Framework.* While Communications Sector companies are promoting cyber risk management, including continued use of the *Framework*, we are awaiting the new version of the *Cybersecurity Framework* to evaluate it and adapt it to the Communications Sector. Sector members and associations are actively involved in the process to update the *Cybersecurity Framework*. Efforts to substantially change the *Framework*, or to promote a more prescriptive approach in other NIST publications, regulations or legislation, may undermine the utility of the *Framework*. We urge NIST to maintain the *Framework* as a stable, central part of cyber risk management, so that companies looking for guidance can rely on it.

CTIA will continue coordinating members and other industry leaders on the security of mobile networks and devices. This includes continued efforts that embody the principles of the *Cybersecurity Framework*, including the extensive research and coordination conducted via the CSWG, and other information sharing efforts and partnering efforts by CSWG and its members with various government agencies through public-private partnerships. This also includes convening members and the public for educational and technical events. Many of these events highlight and promote the *Framework*. For example, CTIA is planning a webinar for its small- and medium-sized carriers and other members, to discuss cybersecurity risk management best practices and use of the *Cybersecurity Framework.*

In November 1017, NTCA plans to release the first issue of the NTCA Cyber Source, a bi-annual cybersecurity publication to keep small, rural telecom providers up-to-date on cybersecurity best practices and emerging topics from subject-matter experts. Further, in 2018, NTCA plans to continue to update and enhance the NTCA Cybersecurity Bundle, as described above, a risk management implementation guide based upon the best practices espoused in the NIST Cybersecurity Framework. The association also plans to continue its extensive educational and training opportunities to assist small telecom operators with bolstering their cyber posture,

including producing its successful NTCA Cybersecurity Summit in October 2018 in Dallas, Texas.

USTelecom just released its 2018 Cybersecurity Toolkit with over 350 links to valuable cybersecurity related resources. The NIST Cybersecurity Framework is prominently featured along with guidance for small and medium business as well as Board of Directors and C-level executives (http://www.ustelecom.org/sites/default/files/documents/2018%20Cybersecurity%20Toolkit%20FINAL%2010-26.ppsx).

GAO QUESTION #3: BASED ON YOUR INTERACTIONS WITH ORGANIZATIONS THAT ARE MEMBERS OF THE COMMUNICATIONS SECTOR, WHAT ARE THE CURRENT USE RATES OF THE *CYBERSECURITY FRAMEWORK*?

a. GAO QUESTION #3A: WHAT ARE SOME OF THE CHALLENGES / BARRIERS TO USING THE *CYBERSECURITY FRAMEWORK* AMONG SECTOR ORGANIZATIONS?

Challenges to use of the *Cybersecurity Framework* include shifting or unclear expectations, changes to the *Cybersecurity Framework* itself, and the resource limits of smaller organizations.

The *Cybersecurity Framework* has been successful in the Communications Sector because it provides a practical risk management approach, which can serve as a reference point for mature security programs. Any move away from this model would erect a barrier to adoption and use. This includes a premature push to make the *Cybersecurity Framework* mandatory for private companies, or to include in Version 1.1 expectations for measurements or metrics related to adoption. If regulatory or other agencies move toward prescriptive regulations for cybersecurity, it could undermine the importance of the *Cybersecurity Framework* and reduce interest in using it. For example, government policymakers concerned about security should look to the *Framework*'s risk management approach and avoid over-inclusive or prescriptive obligations that treat different risks or products all the same.

There is concern about how updates to the *Cybersecurity Framework* could affect uptake and use. For example, there may be interest in incorporating distinct privacy concepts into the *Cybersecurity Framework* or some of its informative references, as is the case with NIST SP 800-53, which is currently being revised to combine privacy and security. Any additions to the complexity of the *Cybersecurity Framework* threaten to undermine its utility and adoption.

Finally, small- and medium-sized businesses in the Communications Sector have faced challenges in addressing cybersecurity, from use of the *Cybersecurity Framework* to participating in information sharing. In small- and medium-sized businesses, the IT security function may be managed by individuals or departments that have several responsibilities and relatively limited resources. As the *CSRIC IV Report* explained, "[w]hile for large organizations the cybersecurity practices outlined in the NIST Framework would largely be considered just a cost of doing business, the majority of small to medium-sized organizations would view these

as costs with no calculable direct return on investment."[41] This is why efforts focused in the CSRIC on small- and medium-size members, and have worked to promote it to them. It is also why the *CSRIC IV Report* focused on mitigating costs that disproportionately impact small- and medium-sized businesses. More can be done to promote cyber risk management among small- and medium-sized organizations. In fact, government efforts, like those at NIST, might focus on this segment with use cases and other work, instead of regularly updating existing documents or promulgating new guidance.

b. GAO QUESTION #3B: WHAT ARE SOME OF THE KEY SUCCESSES / FAILURES AMONGST SECTOR MEMBERS WITH RESPECT TO THE CURRENT USE OF THE CYBERSECURITY FRAMEWORK?

The Communications Sector is using the *Cybersecurity Framework* as designed. It is used as a starting point for cybersecurity risk management, not an end state. The *Cybersecurity Framework* complements communications companies' cybersecurity programs, drawing on practices from various standards bodies. The *Cybersecurity Framework* is helping organizations manage risk, and it is spurring the creation of derivative cybersecurity approaches as companies, associations, standards bodies and non-U.S. governments look to it for guidance.

The *Cybersecurity Framework* has proven to be particularly useful in providing a common taxonomy for stakeholders to identify, analyze, and map existing practices and standards. In the Communications Sector, all players—from carriers to Operating System ("OS") providers and developers, from manufacturers to applications developers—must contribute to security. As a practical example, in the wireless and Internet ecosystems, this means that Operating System ("OS") providers work with application developers; OS application stores screen applications; network operators monitor traffic and combat threats; and over-the-top applications add security. One common taxonomy is a useful tool in this multi-layered, complex system of systems.

The *Cybersecurity Framework* Core has proven to be especially helpful because it provides activities to achieve specific outcomes, and identifies available standards and guidance that can help achieve those outcomes. As part of the mapping process that contributed to the *CSRIC IV Report*, the Wireless Segment Subgroup found that the *Framework* Core Functions, Categories, and Subcategories were particularly useful for articulating outcomes and illustrating use-case scenarios for wireless technologies, networks, and services.

The *Cybersecurity Framework* has become a baseline for sector efforts, facilitating dialogue and action *across sectors*. NIST itself lists over 50 documents and tools that incorporate or help to implement the *Cybersecurity Framework*, a primary example of which is the *CSRIC IV Report* that maps the *Cybersecurity Framework* to the Communications Sector. The *Cybersecurity Framework* has also become a baseline for international efforts.

Individual companies have noted their use of the *Cybersecurity Framework* and its complementary utility.

- AT&T "employ[s] a cybersecurity risk management program that predates the *Framework*. [They] currently have an internal security policy based upon widely

[41] CSRIC IV Final Report at 204.

accepted, international security standards, such as ISO 27001, PCI, SAS/70, and NIST 800-53. Many of these standards mirror the informative references included in the Framework. [They] use these standards to inform [their] internal controls that [they] then apply to our network systems and in protecting customer data. Thus, the Framework serves as a complement to that program."[42]

- iconectiv has said that "the major benefit of the Voluntary Risk Management Framework is that it can be applied to different business models, technologies and applications. It creates a uniform structure to characterize controls and identify residual risks, emphasizing outcomes and adaptation to evolving threats. It, appropriately, avoids revisiting privacy and other specific security controls already dealt with in other vehicles. It acknowledges that one risk management solution does not fit the variety of critical infrastructure providers and associated technologies and services."[43]

Overall, the Communications Sector has observed successes with respect to the use of the *Cybersecurity Framework*. CSCC counts as a success the collaborative sector-wide effort to map the *Cybersecurity Framework* in CSRIC.

GAO QUESTION #4: WHAT EFFORTS HAVE BEEN TAKEN TO DETERMINE THE CURRENT LEVEL OF USE OF THE CYBERSECURITY FRAMEWORK AMONG COMMUNICATIONS SECTOR MEMBER ORGANIZATIONS?

Each CSCC participant encourages its members to exchange best practices about cybersecurity and use the *Framework* as they see fit, consistent with its voluntary, flexible approach. GAO should understand that measuring level of "use of the Cybersecurity Framework" is not a proxy for security or preparedness. Organizations can be quite good at security without formally using the *Cybersecurity Framework*; conversely, "use" of the Framework will not improve security if the choices, policies, and actions of a company in implementing its various approaches do not create repeatable, effective security for its environment. It would not be a good use of resources to focus too closely on measuring "use of the *Cybersecurity Framework*."

Individual associations conduct their own efforts to support members' cybersecurity needs. For example, to the extent CTIA has a need to understand its members' experiences with the *Cybersecurity Framework*, CTIA relies on self-reporting and independent surveys.[44] For example, Cisco, publishes an Annual Cybersecurity Report, which, among other things, looks at the *Cybersecurity Framework:* the Cisco 2017 Security Capabilities Benchmark Study reports that 28% of organizations require vendors to use the *Cybersecurity Framework*.[45] Additionally,

---

[42] AT&T Comments to NIST (Feb. 23, 2016), https://www.nist.gov/sites/default/files/documents/2017/02/14/20160223_att.pdf.

[43] Iconectiv Comments to NIST (Feb. 23, 2016), https://www.nist.gov/sites/default/files/documents/2017/02/13/20160208_iconectiv.pdf.

[44] *See, e.g., Gary Stoller, Few adopt NIST cybersecurity guidelines, but that could change, ThirdCertainty (Apr. 11, 2016),* http://thirdcertainty.com/featured-story/few-adopt-nist-cybersecurity-guidelines-but-that-could-change/*; Melanie Watson, Top 4 cybersecurity frameworks, IT Governance, (Mar. 15, 2017) (noting that the NIST Framework is currently the fourth most widely adopted framework), available at* https://www.itgovernanceusa.com/blog/top-4-cybersecurity-frameworks/.

[45] Cisco 2017 Annual Cybersecurity Report.

CTIA has filed numerous comments on the *Framework*, which have drawn on members' use and individual experiences.

USTelecom conducted a confidential survey of member use of the *Cybersecurity Framework* in 2015 and used the information to develop a series of workshops for our members reviewing the operational and technical requirements associated with each of the 98 sub-categories. This survey was based on assurances of strict confidentiality.

GAO QUESTION #5: WHAT EFFORTS HAVE BEEN TAKEN TO DETERMINE ORGANIZATIONS' SUCCESS IN MITIGATING CYBERSECURITY RISK USING THE CYBERSECURITY FRAMEWORK? WHAT HAVE BEEN THE RESULTS?

CSCC members regularly evaluate their own cybersecurity risk mitigation, and have applied and used the *Cybersecurity Framework*. Some associations conduct their own efforts to identify trends and usage of various tools.

- USTelecom notes that by its design, the CSF is intended to be a flexible tool for companies to implement, evaluate or enhance their cybersecurity risk management programs. Companies have been advised and encouraged to use the CSF in ways they determine to be beneficial and have been assured that measuring implementation and any associated reporting would not be used as a basis for determining the effectiveness of the CSF. As presented in the WG IV report and in our sector efforts to reframe the CSF 1.1 update discussion on metrics, any measurement effort may be conducted at the enterprise level and should not be subject to any reporting requirements that are likely to chill the use of the voluntary framework. Accordingly, the sector has refrained from any organized activity to test "adoption," but has instead focused its efforts on making the "use" of the Framework more attractive and understandable to companies.

- CTIA's CSWG conducts industry-wide research on a regular basis to assess the relative security of networks and to identify both gaps and best practices. CTIA see Communications Sector members engaged in effective, aggressive mitigations of cybersecurity risk, using various approaches and tools. Currently, the CSWG is conducting studies regarding cybersecurity threats to the IoT, vulnerabilities of the developing 5G network, and TDoS attacks. The studies are designed with risk management—as embodied in the *Framework*—in mind, and therefore, the analysis from the studies reflects the basic principles on which the *Framework* is based. This research helps to inform the wireless segment on its success in mitigating cybersecurity risk. Due to the highly sensitive nature of networks, the current threat environment in which we operate, and legal issues related to competition, the results of these studies are non-attributable and aggregated.

GAO QUESTION #6: DOES THE COMMUNICATIONS SECTOR HAVE ANY QUALITATIVE OR QUANTITATIVE MEANS FOR MEASURING IMPLEMENTATION OF THE FRAMEWORK?

Cybersecurity is inherently difficult to measure for many reasons. *First*, Cybersecurity is not an exact science and does not lend itself well to exact measurement. *Second*, cause and effect are difficult to pinpoint, as inputs (*e.g.*, security training, access controls, firewalls, and other various protective controls) are significantly separated in time from outputs (*e.g.*, a cybersecurity event, or lack thereof). Effective cybersecurity may be reflected in the *avoidance* of a harmful practice, attack, or breach. In the same vein, a harmful attack or breach is not always an indication of ineffective cybersecurity measures. Indeed, companies who have suffered high-profile hacks often were viewed as having fairly robust cybersecurity programs. This is why experts are increasingly focusing on *resiliency*, and not on the mere use of the *Cybersecurity Framework* or another approach. There is not consensus on how an organization demonstrates efficacy. *Finally*, every organization is unique, with its own risk environment, risk tolerance, resources, goals (business, cybersecurity, and otherwise), etc. Business objectives in particular are highly variable and evolve over time. Changing business objectives may change cybersecurity objectives.

With this in mind, CSCC members agree that self-assessment of cybersecurity efforts can be helpful to an organization, and is an indication of a mature cyber risk management approach. However, there is not, nor could or should there be, a single qualitative or quantitative approach to measure implementation of the *Cybersecurity Framework* in the Communications Sector. Self-assessments must be voluntary and flexible—a uniform approach would fly in the face of the sound risk management practices that the *Cybersecurity Framework* seeks to promote.

The prudent approach is for companies to measure against numerous benchmarks, vulnerabilities, and data points, selected by each company as relevant to its threat environment, resources, tools, and capabilities. The focus should be on processes and the adequacy of those processes to detect and protect against threats. The *Cybersecurity Framework* is used to inform or complement those processes. Companies self-assess to determine if their overall programs are effective, not whether use of the *Cybersecurity Framework* itself is effective. For self-assessment to be meaningful, it cannot involve simple compliance with a checklist—whether that checklist is the *Cybersecurity Framework* or a set of standards. Self-assessments should ask fundamental questions like "Is the program meeting the risk management needs of the company?" and "Is the program enabling the company to identify and respond to threats?"

****

In sum, we hope that GAO sees the substantial value that the *Cybersecurity Framework* has brought to the Communications Sector, and how impactful it has been. While there are no easy solutions to measuring cybersecurity "success," GAO can readily conclude that the Communications Sector has enthusiastically embraced it and many other cybersecurity risk management tools that are available to help companies identify, manage and mitigate their unique cybersecurity challenges.

Best regards,

COMMUNICATIONS SECTOR COORDINATING COUNCIL

Robert Mayer
Chairman
Communications Sector Coordinating Council

Kathryn Condello
Vice Chairman
Communications Sector Coordinating Council