Federal Communications Commission
Washington, D.C. 20554

April 12, 2013

Via Electronic Mail

Ms. Diane Honeycutt
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland 20899

Dear Ms. Honeycutt:

Please find attached the comments of the Federal Communications Commission's Public Safety and Homeland Security Bureau in Docket No. 130208119–3119–01, "Developing a Framework to Improve Critical Infrastructure Cybersecurity." We welcome the opportunity to comment.

Please feel free to contact me at (202) 418-1300 or by e-mail at david.turetsky@fcc.gov if you have any questions about this submission.

Sincerely,

David S. Turetsky
Chief
Public Safety and Homeland Security Bureau

Comments of
FCC Public Safety and Homeland Security Bureau
NIST Docket Number 130208119–3119–01
"Developing a Framework to Improve Critical Infrastructure Cybersecurity"

Overview

The Federal Communications Commission's (FCC or Commission) Public Safety and Homeland Security Bureau (PSHSB or Bureau) welcomes the opportunity to comment on the Department of Commerce National Institute of Standards and Technology (NIST) Request for Information (RFI)[1] regarding the development of a framework to reduce cyber risks to critical infrastructure. PSHSB is the primary entity within the FCC responsible for developing, recommending, and administering the Commission's policies on public safety issues. These policies include 9-1-1, E9-1-1, Next Generation 9-1-1, operability, and interoperability of public safety communications, communications infrastructure protection and disaster response, network security and reliability, and cybersecurity. The Commission is focused on advancing initiatives that further strengthen and enhance the security and reliability of the Nation's communications infrastructure and public safety and emergency response capabilities. We therefore welcome the opportunity to share our experience gained from addressing some of the most critical public safety communications issues facing the Nation.

As President Obama recognized in his recent Executive Order on Improving Critical Infrastructure Cybersecurity: "[t]he cyber threat to critical infrastructure . . . represents one of the most serious national security challenges we must confront."[2] The security of the Internet is essential to its success as an engine of economic growth, productivity, and social interaction. As society has come to depend on the services and capabilities the Internet enables, the risk of misuse increases, exposing users to fraud, theft, and other malicious activities.

A core element of the FCC's mission is to ensure that communications networks of all types "promot[e] safety of life and property."[3] To this end, the Commission works to ensure the reliability and resiliency of the Nation's communications networks against cyber threats. The FCC fulfills this part of its mission through several means.

---

[1] *See* https://www.federalregister.gov/articles/2013/02/26/2013-04413/developing-a-framework-to-improve-critical-infrastructure-cybersecurity.

[2] Exec. Order No. 13,636, "Improving Critical Infrastructure Cybersecurity," 78 Fed. Reg. 11,739 (Feb. 19, 2013).

[3] 47 U.S.C. § 151.

Engaging Stakeholders. The FCC works with federal partners, broadband providers, and other stakeholders to develop smart, practical, voluntary solutions to address cybersecurity threats. Since 2001, the FCC, through federal advisory committees such as the Network Reliability and Interoperability Council (NRIC)[4] and its successor, the Communications Security, Reliability and Interoperability Council (CSRIC),[5] has pursued an effective multi-stakeholder approach that convenes communications security experts to develop and recommend practical cybersecurity best practices and solutions. CSRIC is composed of over 50 leaders from the private sector, academia, engineering, consumer/community/non-profit organizations, and government partners from tribal, state, local and federal agencies. CSRIC members are appointed by the Chairman of the FCC to provide balanced expertise and viewpoints. It develops recommendations for the FCC using a consensus process in accordance with the Federal Advisory Committee Act.[6] The Chairman, in close cooperation with stakeholders, establishes the goals and objectives for every two-year charter period. Recommendations from CSRIC to the Commission are captured in publicly-available reports, and are revisited periodically as needed.

The FCC began work on cybersecurity-related issues in 2001 through NRIC, and CSRIC continued the work in cybersecurity beginning in 2009. Between 2009 and 2011, CSRIC recommended discrete cybersecurity practices that are applicable to communications providers in their day-to-day methods and procedures. Under the most recent CSRIC charter, which covered the period from March 2011 to March 2013, CSRIC addressed some of the most difficult and intractable problems that afflict the core Internet: (1) secure inter-domain routing, (2) secure domain name system, and (3) botnet remediation. CSRIC brought key stakeholders together in a collaborative, public-private process that resulted in practical recommendations for improvement and, in March 2012, CSRIC unanimously adopted recommendations in all three areas.[7] In March 2013, CSRIC recommended metrics with which to determine the effectiveness of the 2012 improvements. The Bureau is now working to implement data collection and analysis processes for these metrics. Internet service providers (ISPs) representing over 92 percent of the residential broadband subscribers in the U.S. have committed to implement these recommendations. As explained more fully in our responses to specific questions from the RFI below, the targeted, deeply technical work of the CSRIC demonstrates that it is an effective model for the sector-specific development of cybersecurity methods and procedures that will follow the development of the Cybersecurity Framework. This work can also contribute to a strong foundation for success of the communications sector follow-on work. The Commission has announced its intention to recharter CSRIC for another two-year term.[8]

---

[4] The Network Reliability and Interoperability Council was first chartered in 1991.

[5] CSRIC was first chartered in 2007.

[6] *See* 5 U.S.C. App. 2; *see also* http://www.gsa.gov/portal/category/21244.

[7] *See* "FCC Advisory Committee Adopts Recommendations To Minimize Three Major Cyber Threats, Including an Anti-Bot Code of Conduct, IP Route Hijacking Industry Framework and Secure DNS Best Practices," *News Release* (rel. Mar. 22, 2012), *available at* http://www.fcc.gov/document/csric-adopts-recs-minimize-three-major-cyber-threats.

[8] *See* "FCC Announces Intention to Recharter the Communications Security, Reliability, and Interoperability Council for a Fourth Two-Year Term; Seeks Nominations by March 20, 2013 for Membership," *Public Notice*, 28 FCC Rcd 1079 (2013).

The Commission also makes use of other federal advisory committees to make recommendations in the area of cybersecurity, notably the Technological Advisory Council (TAC). The TAC is comprised of a diverse array of leading experts that helps the FCC identify important areas of innovation and develops informed technology policies supporting America's competitiveness and job creation in the global economy. The most recent TAC made recommendations on, among other things, mobile security, including recommendations on how to improve security for both cellular and WiFi networks.[9] In 2013, the TAC has two working groups focusing on cybersecurity-related issues, one addressing network resilience in general, the other on cybersecurity issues posed by the transition of communication services, such as VoIP, to cloud-based services.

Commission staff also participates in industry standards organizations to foster the inclusion of cybersecurity considerations in the system design phase, for example the newly-created Internet Engineering Task Force working group that is addressing spoofing of telephone numbers in VoIP calls.

Consumer Education and Outreach. To fulfill its responsibility to consumers, the FCC provides public outreach, education and resources on communications issues, including the risks and threats of cyber attacks and methods to mitigate these risks. For example, in October 2011, the FCC launched its "Small Biz Cyber Planner," an online resource to help small businesses create customized cybersecurity plans. An updated version was released in October 2012.[10] In December 2012, the Commission launched the "Smartphone Security Checker," an online tool, customized by operating system, that provides consumers with 10 customized steps and tips to help protect their device.[11] The tool is the result of a public-private partnership between government experts, smartphone developers, and private information technology and security companies.[12] The FCC also participates in the inter-agency "Stop. Think. Connect." campaign and the related nationwide effort to promote cybersecurity awareness and education.[13]

Situational Awareness. Regardless of whether communications outages result from natural disasters or man-made events, including cyber attacks, situational awareness about the outages is important in order to prioritize restoration actions and leverage information to prevent future outages. The FCC provides ongoing situational awareness of major communications outages to our federal partners through the Network Outage Reporting System (NORS),[14] which PSHSB designed and administers. In times of disaster, we provide information to our federal partners on

---

[9] *See* http://transition.fcc.gov/bureaus/oet/tac/tacdocs/meeting121012/TAC12-10-12FinalPresentation.pdf (Wireless Security and Privacy Working Group).

[10] *See* http://www.fcc.gov/cyberplanner.

[11] *See* http://www.fcc.gov/smartphone-security.

[12] *See* http://www.fcc.gov/smartphone-security.

[13] *See* http://www.dhs.gov/stopthinkconnect.

[14] *See* http://transition.fcc.gov/pshs/services/cip/nors/nors.html.

operating status and restoration efforts through the voluntary Disaster Information Reporting System (DIRS).[15] Both NORS and DIRS include features that allow communications providers to submit detailed information about the causes of outages, including cyber-related causes. As we evolve our strategies in the area of cybersecurity we will continue to adapt CSRIC recommendations on cybersecurity metrics to improve our reporting capabilities.

Analysis and Response. Working with the National Cybersecurity and Communications Integration Center (NCCIC) at the U.S. Department of Homeland Security (DHS) and other federal partners, the FCC has an increasing role in assisting with the analysis and response of cyber incidents to protect our Nation's communications infrastructure. Two recent examples illustrate the FCC's activity in this area. In February 2013, PSHSB worked with broadcasters and equipment manufacturers to respond quickly to a cyber attack targeting equipment used by broadcasters to receive and transmit national Emergency Alert System (EAS) alerts. EAS equipment at broadcast stations in several states had been hacked to distribute a false alert that "zombies" were rising from the grave. On learning of the cyber incident, PSHSB quickly contacted affected broadcast stations and other EAS stakeholders as well as equipment manufacturers to determine the possible cause and scope of the incident. The Bureau then worked with EAS stakeholders to develop and widely distribute an advisory informing broadcasters and other EAS participants of the steps to take to secure their EAS equipment, and mitigate the possibility of similar incidents. The entire response was accomplished within twenty-four hours of learning of the incident. The integrity and security of the EAS system is critically important to public safety. In this case, it was relatively easy for the public to realize that the message was false. A message falsified in a less obvious way could lead to public panic.

In March 2013, the NCCIC notified the FCC that the public safety community was experiencing crippling Telephony Denial of Service (TDoS) attacks that stemmed from fraudulent "payday loan" collections.[16] Some Public Safety Answering Points (PSAPs) were receiving calls that a fictitious employee owed money. When the PSAP staff told the caller that the named person did not work there and hung up, multiple phone lines in the PSAP began to ring, potentially preventing emergency calls from reaching 9-1-1 call-takers. The originating phone numbers for these calls were being "spoofed" using Voice over Internet Protocol (VoIP) technology, which prevented local officials from blocking incoming calls from the number where the calls originated. The FCC is working with DHS to coordinate with federal partners, public safety, and industry partners, to lessen the impacts of these attacks and to bring together key stakeholders to track and shut down the calls.

The Commission, through PSHSB, is actively participating in the interagency process to effectuate the Executive Order, and we look forward to working with NIST in developing the Framework and with all of our partners in the more detailed work within the communications sector that will follow its release. Below is the Bureau's response to selected questions in the RFI.

---

[15] *See* http://transition.fcc.gov/pshs/services/cip/dirs/dirs.html.

[16] *See* http://nakedsecurity.sophos.com/2013/04/03/tdos-attacks-target-emergency-call-centers/.

Responses

Part I. Current Risk Management Practices

NIST solicits information about how organizations assess risk; how cybersecurity factors into that risk assessment; the current usage of existing cybersecurity frameworks, standards, and guidelines; and other management practices related to cybersecurity. NIST is interested in understanding whether particular frameworks, standards, guidelines, and/or best practices are mandated by legal or regulatory requirements and the challenges organizations perceive in meeting such requirements.

1. ***What do organizations see as the greatest challenges in improving cybersecurity practices across critical infrastructure?***

There are at least six major actions necessary to improve cybersecurity practices across critical infrastructure components:

(1) Establishing a baseline set of voluntary cybersecurity best practices for application across the set of stakeholders that span the Internet ecosystem, and ranging from protocol design and system architecture to software engineering practices and network operations;
(2) Defining metrics, along with measurement systems, and obtaining data with which to measure improvements in the cybersecurity practices relative to the benchmarks;
(3) Improving cybersecurity practices in the face of the ever-changing cybersecurity vulnerabilities, threats, and exploits used by sophisticated adversaries;
(4) Providing incentives to all Internet system stakeholders to improve cybersecurity practices;
(5) Incorporating Supply Chain Risk Management (SCRM) into the cybersecurity practices; and
(6) Expanding cybersecurity education across all critical infrastructure sectors.

Objective metrics are a key input to all of these actions, and critical infrastructure sectors and federal agencies need to work cooperatively to establish, collect, and share these metrics to drive continuous improvement in cybersecurity. Metrics will be necessary as a basis for determining the effectiveness of improvement initiatives and guiding additional efforts. The lack of consistent, meaningful, and widely-applicable baseline metrics to assess the current national cybersecurity posture is a major challenge to improving cybersecurity practices across the critical infrastructure sectors.

The Commission's work with NORS, DIRS and the measurement activities associated with the CSRIC provide us with experience both in convening stakeholders to define sector-specific cybersecurity best practices and the metrics to help determine their effectiveness and improve them over time. This experience can be leveraged to support the development of the Cybersecurity Framework and in subsequent sector-specific initiatives. These contributions and

capabilities can serve as a model for the follow-on work that will be required to implement the Framework and are further described in our responses to subsequent questions.

2. ***What do organizations see as the greatest challenges in developing a cross-sector standards-based Framework for critical infrastructure?***

The greatest challenge to developing a cross-sector standards-based Framework is the relative lack of experience that relevant sectors have in working together on cybersecurity issues. Most often, each sector works individually to address cybersecurity challenges within its own sphere. It is inherently difficult for a group with diverse cyber security threats to develop a common framework to apply across many sectors.

One way to avoid this outcome is to have the process driven by an overarching strategic set of principles. The cross-sector *National Strategy to Secure Cyberspace*[17] *(National Strategy)* and the DHS *Blueprint for a Secure Cyber Future*[18] *(Blueprint)* are good sources for this purpose. Clarifying the relationship between and application of the *National Strategy* and/or the *Blueprint* to the Framework will provide consistent overarching policies to govern the development, implementation, and measurement of the effectiveness of the Framework and create a linkage to the significant work that has already been done.

For example, guided by many of the National Cyberspace Security Priorities listed in the *National Strategy* and the *Blueprint*, communications service providers and organizations such as those members of the FCC's CSRIC, have taken positive steps towards identifying and implementing voluntary cybersecurity best practices to address specific, critical cybersecurity threats and vulnerabilities like domain name fraud, Internet route hijacking, and botnets. These efforts should be leveraged, both in methodology and in substance, to address many of the anticipated challenges in developing the Framework for critical infrastructure and the sector specific initiatives that will follow release of the Framework.

3. ***Describe your organization's policies and procedures governing risk generally and cybersecurity risk specifically. How does senior management communicate and oversee these policies and procedures?***

The FCC's Office of Managing Director (OMD) has standard procedures that specify how cybersecurity risks are managed within the FCC. Offices within OMD monitor cybersecurity risks and develop risk mitigation tactics for the FCC's network and information systems. These tactics include the use of cybersecurity defense tools such as Intrusion Detection Systems and Host-Based Security Systems.

---

[17] *See* http://confluence.senki.org/download/attachments/1769488/65_NationalStrategytoProtectCyberspace.pdf?version=1&modificationDate=1333740384920.

[18] *See* http://www.dhs.gov/blueprint-secure-cyber-future.

4. Where do organizations locate their cybersecurity risk management program/office?

The FCC's cybersecurity program, led by the Chief Information Security Officer, includes the Network Security Operations Center and the Cybersecurity Compliance, Audit, and Policy branches. These elements are part of the FCC's Information Technology Center, led by the Chief Information Officer. The Information Technology Center is an arm of OMD, which is responsible for the Commission's administrative functions.

8. What are the current regulatory and regulatory reporting requirements in the United States (e.g. local, state, national, and other) for organizations relating to cybersecurity?

The FCC does not impose mandatory reporting requirements with respect to broadband services, except that, as of December 16, 2012, significant disruptions of interconnected VoIP services must be reported.[19] Voluntary reporting on the condition of broadband services during major emergencies occurs through the FCC's Disaster Information Reporting System. CSRIC has recommended a number of cybersecurity voluntary measures that involve information exchange, but these recommendations have not included reporting directly to the FCC. Each of these is discussed below.

Voluntary Cybersecurity Best Practices Developed Through CSRIC. CSRIC has produced industry-based, voluntary best practices that address major Internet security vulnerabilities: the Domain Name System (DNS), inter-domain routing security, and bots in residential networks that result in malware and allow distributed denial of service (DDoS) attacks.[20] CSRIC followed this work with recommendations concerning appropriate measures of effectiveness for the best practices. These measurement recommendations were delivered in March 2013, and the FCC's process for collecting the information and analyzing the associated data remains in the early stages. Technically sophisticated, multi-stakeholder work, such as that of CSRIC, could be leveraged to help implement the sector-specific processes that will follow the release of the Framework.

Measurement Infrastructure. As part of the *Measuring Broadband America* initiative,[21] the Commission has deployed, by contract, more than 8,000 measurement devices to residential broadband consumers. These devices have been used primarily to measure network performance, such as throughput and delay, and also offer an infrastructure to observe cybersecurity-related metrics, such as the extent of DNSSEC deployment.

Mandatory Reporting of Communications Outages. Cybersecurity events can lead to localized or large-scale outages, and, in turn, resilient network design limits the impact of such events.

---

[19] *See* 47 C.F.R. § 4.9(g).

[20] *See* Reports from CSRIC Working Groups 5, 6, and 7 *available at* http://www.fcc.gov/encyclopedia/communications-security-reliability-and-interoperability-council-iii.

[21] *See* http://www.fcc.gov/measuring-broadband-america.

The FCC requires communications providers to report disruptions to communications that exceed certain thresholds to wireline, wireless, cable, interconnected VoIP, and satellite communications. The data is submitted into the NORS database, and the Commission works in close coordination with communications providers and DHS to address long-term and imminent communications reliability issues.[22] The data can reveal a causal link between a cyber event and a physical, transport, or service layer consequence, which can be helpful in identifying points of failure when disruptions to communications occur. While we have not seen a tie between cyber and physical outages to-date, we expect that could change with the recent addition of interconnected VoIP outage reporting. For example, according to press reports a massive DDoS attack over several days in March 2011 brought down the VoIP call-processing supplied by TelePacific Communications to many of its customers.[23] TelePacific serves about 1.2 million access lines. The massive DDoS attack resulted in widespread service disruptions and, according to press reports, cost the VoIP provider hundreds of thousands of dollars in customer credits. This event would be reportable under the FCC's current rules adopted in December 2012 where VoIP outages lasting longer than thirty minutes and affecting 900,000 user-minutes are reportable.

Voluntary Reporting of Communications Status During Major Disasters. During major disasters, the FCC collects information, provided on a voluntary basis by service providers, on the operating status and restoration efforts of a wide range of communications services, including broadband services.[24] DIRS collects information on physical and transport outages, but can also offer information about cyber root causes. In the short term, the FCC uses DIRS information to aid in restoration efforts and, in the long term, for analysis of weaknesses in the system and ways to improve overall resiliency and reliability.

Information from both NORS and DIRS is shared with the NCCIC and used, as appropriate, with communications providers to identify and resolve communications reliability issues. Over the years, this process has led to data-driven continuous improvement resulting in a number of measurable, successful interventions, all implemented through voluntary cooperation with communications providers. For example, shortly after the outage reporting rules became effective, the Commission noticed an upward trend in the incidence of high-capacity transport facility outages. The Commission referred this issue to the Alliance for Telecommunications Industry Solutions (ATIS), which developed revisions to existing best practices, which helped to reverse the trend and reduce the number of outages.

In a more recent case, the Commission observed an unacceptable upward trend in "hard down" wireline outages. Using NORS data and working on a systematic basis with the ATIS Network Reliability Steering Committee (NRSC), the Bureau identified and analyzed trends and possible

---

[22] Under FCC rules and precedent, the data submitted is presumed confidential and shared only with DHS. *See* 47 C.F.R. § 4.2; New Part 4 of the Commission's Rules Concerning Disruptions to Communications, *Report and Order and Further Notice of Proposed Rule Making*, ET Docket No. 04-35, 19 FCC Rcd 16830, 16856 ¶47 (2004).

[23] *See* http://www.networkworld.com/news/2011/100411-ddos-voip-251553.html?page=3.

[24] Data submitted into DIRS is also presumed confidential and shared only with DHS. *See* The FCC's Public Safety & Homeland Security Bureau Launches Disaster Information Reporting System (DIRS), *Public Notice*, 22 FCC Rcd 16757 (PSHSB 2007).

causes of the outages in provider networks across the industry. With the benefit of the Bureau's analysis and additional work of the NRSC, providers were able to correct problems that reduced the incidence of these outages by over forty percent.[25] This was possible because the Commission, as the central collection point for outage information from individual providers, has the ability to piece together the overall picture of network performance across the industry by analyzing NORS data and sharing aggregated data with industry network experts.

This work, and other similar analyses of NORS, had a significant, positive effect on public safety. In a "hard down" outage, for example, no calls complete, including calls to 9-1-1. Reducing these and other types of outages significantly improved the ability of the public to reach emergency help. As 9-1-1 service continues to evolve toward a packet-switched environment, new "Next Generation 9-1-1" services will rely increasingly on broadband services. The ability to analyze and respond to outages, particularly those emanating from cyber attacks, will be a critical element of maintaining the public's ability to call for help.

Part II. Use of Frameworks, Standards, Guidelines, and Best Practices

As set forth in the Executive Order, the Framework will consist of standards, guidelines, and/or best practices that promote the protection of information and information systems supporting organizational missions and business functions. NIST seeks comment on the applicability of existing publications to address cybersecurity needs, including, but not limited to, the documents developed by: international standards organizations; U.S. government agencies and organizations; state regulators or public utility commissions; industry and industry associations; other Governments, and non-profits and other non-government organizations.
NIST also seeks information on the current usage of these existing approaches throughout industry, the robustness and applicability of these frameworks and standards, and what would encourage their increased usage.

1. What additional approaches already exist?

Since 1991, the FCC, through federal advisory committees such as the NRIC, has pursued an effective, public-private, multi-stakeholder approach to network reliability that convenes communications experts to develop and recommend practical best practices and solutions. Starting in 2001, NRIC's portfolio expanded to include the development of best practices to improve cybersecurity. In 2009, CSRIC began to focus on the development of discrete practices that can be applied by communications providers in their day-to-day methods and procedures. Since 2011, CSRIC has tackled some of the most difficult and intractable problems that afflict the core Internet: secure inter-domain routing, secure domain name system, and botnet remediation. CSRIC's March 2012 and March 2013 recommendations, which focus on the technical and operational improvements to communications sector cybersecurity, can be

[25] *See* Extension of Part 4 of the Commission's Rules Regarding Outage Reporting to Interconnected Voice Over Internet Protocol Service Providers and Broadband Internet Service Providers, *Notice of Proposed Rulemaking*, PS Docket No. 11-82, 26 FCC Rcd 7166, 7171-72 para. 16 (2011).

leveraged to support the more granular, sector-specific activities that will follow release of the Framework.

Domain Name System Security. The danger of domain name fraud can be illustrated by a 2009 incident where the customers of one of Brazil's biggest banks were directed to a fake site that looked exactly like the real one. Customers' user names and passwords were stolen for four hours until the crime was discovered.[26] CSRIC started working on this problem in March 2011, and, in March 2012, CSRIC adopted recommendations for phased deployment of DNSSEC[27] by ISPs.[28] This was followed in March 2013 by recommended metrics for gauging the effectiveness of DNSSEC deployment to protect consumers by reducing domain name fraud caused by cache poisoning and weaknesses in existing DNS protocols.[29] CSRIC recommended that the FCC encourage ISP participation in tests for discovering and characterizing the level of DNSSEC support across the Internet and called for the FCC to encourage the continued deployment of DNSSEC by ISPs and other members of the Internet ecosystem. Going forward, the group recommended that the FCC facilitate an examination of DDoS attacks[30] with the goal of developing possible defensive solutions.

Inter-domain Routing. The Internet is a collection of autonomously administered networks that adhere to a common protocol called Border Gateway Protocol (BGP), which enables seamless, global connectivity. BGP has no built-in mechanisms to protect against attacks that modify, delete, or forge data. When BGP vulnerabilities are exploited, Internet traffic is misdirected and potentially exposed to eavesdropping. In its 2010 report to Congress, the U.S.-China Economic and Security Review Commission described a June 2010 incident that illustrates the importance of secure inter-domain routing: Internet traffic destined for networks around the world was diverted through China before it was forwarded to the correct destination. During the 18 minutes that this exploit lasted, unauthorized networks had visibility of nearly 15 percent of the total internet traffic. Diverting traffic in this manner could have enabled the contents to be recorded, which may have resulted in losses to individuals and private companies and posed a significant threat to national security.[31]

In March 2012, CSRIC recommended a framework that allows industry to incrementally implement standardized, secure routing procedures to address existing weaknesses in the

---

[26] *See* http://www.eweek.com/c/a/Security/Report-Claims-DNS-Cache-Poisoning-Attack-Against-Brazilian-Bank-and-ISP-761709/

[27] "DNSSEC" is a set of extensions to the domain name system protocols that use digital signatures to protect recursive resolvers from falsified DNS data.

[28] *See* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG5-Final-Report.pdf.

[29] *See* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG5_Report_March_%202013.pdf.

[30] *See* http://www.infoworld.com/t/security/fix-your-dns-servers-or-risk-aiding-ddos-attacks-215510. Open DNS resolvers can enable a technique called "DNS amplification" wherein attackers bombard target servers with as much as 100 bytes of network-clogging traffic for every one byte they send out.

[31] *See* http://origin.www.uscc.gov/sites/default/files/annual_reports/2010-Report-to-Congress.pdf, page 236.

Internet inter-domain routing infrastructure.[32] The secure Border Gateway Protocol and Resource Public Key Infrastructure standards establish a registry that enables ISPs to validate the authenticity of routing information, securing the foundations of trust between networks. The final report also provided metrics for measuring progress to ensure that efforts are effective in improving routing security.[33]

Botnet Remediation. Botnets are vast numbers of computers (bots) infected with malicious software. Historically, most of the infected computers were operated by residential users who have little experience or knowledge in cybersecurity and, more than likely, would not know their computer is infected. In a botnet launch, an attacker uses a network of compromised computers (often referred to as zombies) to send millions of simultaneous requests to a target website. The target site becomes overwhelmed, leading to denial of service for legitimate site visitors.

In March 2012, CSRIC recommended a voluntary U.S. Anti-Bot Code of Conduct for Internet Service Providers (ABCs for ISPs) that will help mitigate the botnet threat.[34] In March 2013, CSRIC followed with a final report[35] containing recommendations to facilitate case studies, leverage industry pilot programs, facilitate research in metrics, and foster ongoing dialogue around the subject of metrics. The Working Group's final report,[36] adopted by CSRIC, also addresses barriers to stakeholder implementation of the voluntary best practices comprising the ABCs for ISPs. The development of the Framework and incentives for program participation should address and seek to overcome these barriers.

Developing recommendations through a public-private, multi-stakeholder process such as CSRIC has proved an effective means for creating voluntary frameworks for combatting cyber threats. This approach, and the work done to date through CSRIC, serves as a useful foundation in the development and implementation of the Framework. As CSRIC convenes a large set of industry experts and has an established operating mode, it can tackle specific issues in technical depth and can easily update recommendations to address changing threats, feedback from operational practice and changes in technology capabilities.

2. Which of these approaches apply across sectors?

As discussed above, the public-private multi-stakeholder process that CSRIC and its predecessors have followed since 1991, including with respect to cybersecurity, can apply to any sector. In this model, practitioners and experts from both the private and public sectors are gathered in a trusting, collaborative environment to address specific technical and operational

---

[32] *See* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG6-Final-Report.pdf.

[33] *See* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG6_Report_March_%202013.pdf.

[34] *See* http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC-III-WG7-Final-Report.pdf.

[35] *See* http://www.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG7_Report_March_%202013.pdf.

[36] *Id.*

problems that they share. While the substance of the NRIC and the CSRIC are sector-specific, the methodology is not.

3. Which organizations use these approaches?

The communications sector has used the NRIC/CSRIC approach for over twenty years. The voluntary best practices that have resulted, including those with respect to cybersecurity, have been developed primarily by industry, which makes their application more likely than those developed without significant industry input. The FCC works closely with industry to promote the implementation of the best practices developed through NRIC/CSRIC. The Commission also works with industry on the development of metrics to determine the effectiveness of the best practices in improving and sustaining the reliability and robustness of the Nation's communications networks.

4. What, if any, are the limitations of using such approaches?

The limitations of a voluntary best practices approach is the inability to ensure that the practices are being implemented. Understanding the extent to which providers are implementing best practices, and therefore how well the practices are helping achieve greater network security and reliability, requires the ability to measure service reliability outcomes.[37] With respect to CSRIC, the cybersecurity best practices were only recently adopted, and the Commission continues to work with CSRIC on the development of measurements to determine the overall success of and areas for improvement within the best practices. So far, CSRIC has focused on operational practices, such as the deployment of existing industry standards, but we recognize that software engineering practices are also major factors in improving cybersecurity.

5. What, if any, modifications could make these approaches more useful?

The public-private, multi-stakeholder approached used in NRIC/CSRIC has been effective. The Commission continues to work with CSRIC on addressing barriers to implementation of best practice and the development of metrics that will provide insight into how well the best practices are achieving their purpose. In addition, we would expect that the establishment of a national cybersecurity framework would permit us to better coordinate CSRIC's activities with these goals.

6. How do these approaches take into account sector-specific needs?

The FCC is focused specifically on the communications sector, but our work encompasses a broad range of stakeholders that depend on the sector: communications service providers and network operators; public safety agencies; equipment manufacturers; critical infrastructure providers; and consumers. As appropriate, our work takes into account the needs of other

[37] The Bureau's recent report on the impact of the June 2012 Derecho storm on communications illustrates the limitations of relying exclusively on voluntary best practices. *See* "Impact of the June 2012 Derecho on Communications Networks and Service," Report and Recommendations, rel. Jan. 10, 2013 (PSHSB).

sectors. For example, CSRIC members have included representatives of energy utility companies, financial institutions, and large enterprise users, such as PayPal. The needs of each stakeholder group vary, and the federal advisory committee process used in CSRIC is structured to incorporate a range of relevant interests and to balance viewpoints in the development of recommendations. This public-private, multi-stakeholder approach could easily be adapted by other sectors.

7. ***When using an existing framework, should there be a related sector-specific standards development process or voluntary program?***

The development of an overarching Framework should not foreclose sector-specific work in the interim intended to address cybersecurity challenges. In the communications sector, for example, many cybersecurity threats have been known for years and still remain only partially solved. Problems like inter-domain routing security, DNS security, denial of service attacks, and the proliferation of botnets do not have binary fixes; they respond to relentless, continuous improvements. The current absence of a Framework makes these challenges no less compelling, and continuing ongoing work on them is only likely to advance the larger, cross-sector goals that the Framework is intended to pursue once the Framework is available.

8. ***What can the role of sector-specific agencies and related sector coordinating councils be in developing and promoting the use of these approaches?***

The FCC's experience described above reflects that sector specific efforts that include expert stakeholders to develop collaborative solutions to difficult problems can be effective.

Part III. Specific Industry Practices

In addition to the approaches described above, NIST is interested in identifying core practices that are broadly applicable across sectors and throughout industry. NIST seeks information on the adoption of the following practices as they pertain to critical infrastructure components:

- Separation of business from operational systems;
- Use of encryption and key management;
- Identification and authorization of users accessing systems;
- Asset identification and management;
- Monitoring and incident detection tools and capabilities;
- Incident handling policies and procedures;
- Mission/system resiliency practices;
- Security engineering practices;
- Privacy and civil liberties protection.

12. In addition to the practices noted above, are there other core practices that should be considered for inclusion in the Framework?

Core practices related to supply chain risk management (SCRM) should be included in the framework. SCRM and threats to the supply chain across the critical infrastructures are a significant concern and have been for some time. In response to the most recent threats, the White House released the *National Strategy for Global Supply Chain Security*.[38] The strategy recognizes that disruptions to supply chains caused by natural disasters as well as cyber attacks can adversely impact global economic growth and productivity, stating: "The global system relies upon an interconnected web of transportation infrastructure and pathways, information technology, and cyber and energy networks. While these interdependencies promote economic activity they also serve to propagate risk across a wide geographic area or industry that arises from a local or regional disruption."[39] The FCC shares the growing concern that the communications sector's supply chain risks could compromise the Nation's ability to protect the critical infrastructure on which the government functions and our society depends. It is unlikely that existing SCRM standards are sufficient to address the procedural, contractual, physical, and technical measures required within the communications sector. Closing the gap between existing SCRM standards/best practices and those that are needed can be accomplished by strengthening security controls relating to how communication systems are designed, integrated, and updated and/or improving communication systems acquisition risk management practices. Given the strong interdependency of other critical infrastructures on the communications sector, SCRM core practices should be included in the Framework.

Conclusion

The greatest challenge to developing a cross-sector, standards-based Framework is the relative lack of experience that relevant sectors have in working together on cybersecurity issues, which has the potential to push the Framework toward a greater level of abstraction to accommodate the diverse interests to be considered. Defining objective metrics along with measurement infrastructure to drive continuous improvement, staying ahead of the every-changing nature of the threat, providing incentives to stakeholders to participate in the improvement, and addressing Supply Chain Risk Management should be key elements of the Framework.

The FCC is focused on advancing initiatives that strengthen the security and reliability of the Nation's communications infrastructure and emergency response capabilities and has a long history of engaging in voluntary public-private, multi-stakeholder processes to develop recommendations and policies to this end. Through these processes, the FCC has addressed issues related to communications reliability for over twenty years and cybersecurity for over ten years.

---

[38] *See* http://www.whitehouse.gov/sites/default/files/national_strategy_for_global_supply_chain_security.pdf.

[39] *Id.*

The FCC has significant experience with the operational aspects of security in communications networks as well as with assessing network and service failures and disaster recovery. Combined with well-developed stakeholder relationships that include the communications sector, public safety community, and consumer/community organizations, the FCC is well-positioned to facilitate network reliability improvements and contribute to the process to effectuate the Executive Order. The FCC welcomes the opportunity to participate in the development and implementation of the Framework and encourages NIST to leverage the FCC's expertise and experience, and the significant body of work developed through the public-private, multi-stakeholder CSRIC process to inform sector-specific development and implementation of the Framework.