Before the
Federal Communications Commission

Washington, D.C. 20554

In the Matter of	)	
	)	
Fifth Generation Wireless Network and Device Security	)	PS Docket No. 16-353
	)	

NOTICE OF INQUIRY

Adopted: December 16, 2016 Released: December 16, 2016

Comment Date: [90 DAYS AFTER PUBLICATION IN FEDERAL REGISTER]
Reply Comment Date: [120 DAYS AFTER PUBLICATION IN FEDERAL REGISTER]

By the Chief, Public Safety and Homeland Security Bureau

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION AND BACKGROUND 1
II. INQUIRY 6
A. Protecting Confidentiality, Integrity, and Availability 9
1. Authentication 11
2. Encryption 12
3. Physical Security 16
4. Device Security 19
5. Protecting 5G Networks from DoS and DDoS Attacks 20
6. Patch Management 22
7. Risk Segmentation 26
B. Additional 5G Considerations 32
1. Overview 32
2. Roles and Responsibilities 37
3. Other Considerations 40
4. Benefits and Costs 41
C. 5G Implications for Public Safety 43
III. PROCEDURAL MATTERS 45
A. *Ex Parte* Rules 45
B. Comment Period and Procedures 46
C. Accessible Formats 47
D. Further Information 48
IV. ORDERING CLAUSES 49

I. INTRODUCTION AND BACKGROUND

1. Fifth generation (5G) wireless technologies represent the next evolutionary step in wireless communications. These networks promise to enable or support a diverse range of new applications, and will provide for a vast array of user requirements, traffic types, and connected devices. 5G communications technology could be particularly useful in enabling the growing number of high-capacity networks necessary for transformative business and consumer services, as well as backhaul, and communications related to the "Internet of Things" (IoT) technology.[1]

2. 5G has the potential to be an enormous driver of economic activity. It is a national priority to foster an environment in which 5G can be developed and deployed across the country. That means both ensuring that networks are secure and that the regulatory obligations are measured. We have an opportunity at this stage to ensure that these new technologies and networks are secure by design. Therefore, while the Commission is moving quickly to make the spectrum needed for 5G available in the near term,[2] it is also seeking to accelerate the dialogue around the critical importance of the early incorporation of cybersecurity protections in 5G networks, services, and devices.

3. In its July 2016 *Spectrum Frontiers Report and Order*, the Commission reiterated its view that communications providers are generally in the best position to evaluate and address security risks to network operations.[3] Toward this end, the Commission adopted a rule requiring Upper Microwave Flexible Use Service licensees to submit general statements of their network security plans. The statements are designed to encourage licensees to consider security in their new 5G networks.[4] The statements will also keep the Commission informed of ongoing progress in 5G cybersecurity. The Public Safety and Homeland Security Bureau (PSHSB) issues this Notice of Inquiry (NOI) to seek input on the

---

[1] Significantly, 5G networks, through a combination of cellular, wireless LAN and wired LAN technologies, will support an unprecedented web of connectivity and serve as the central platform for the full, robust deployment of IoT. *See*, *e.g.*, *Machine to Machine (M2M) Market Global Forecast & Analysis*, Markets and Markets, http://www.marketsandmarkets.com/Market-Reports/machine-to-machine-market-732.html; Bill Detwiler, 71 Percent Say M2M is About Developing New Business Opportunities (Apr. 4, 2013), http://www.zdnet.com/71-percent-say-m2m-is-about-developing-new-business-opportunities-7000009304/.

[2] *See*, *e.g.*, *Use of Spectrum Bands Above 24 GHz For Mobile Radio Services*; *Establishing a More Flexible Framework to Facilitate Satellite Operations in the 27.5-28.35 GHz and 37.5-40 GHz Bands*; *Petition for Rulemaking of the Fixed Wireless Communications Coalition to Create Service Rules for the 42-43.5 GHz Band*; *Amendment of Parts 1, 22, 24, 27, 74, 80, 90, 95, and 101 To Establish Uniform License Renewal, Discontinuance of Operation, and Geographic Partitioning and Spectrum Disaggregation Rules and Policies for Certain Wireless Radio Services*; *Allocation and Designation of Spectrum for Fixed-Satellite Services in the 37.5-38.5 GHz, 40.5-41.5 GHz and 48.2-50.2 GHz Frequency Bands; Allocation of Spectrum to Upgrade Fixed and Mobile Allocations in the 40.5-42.5 GHz Frequency Band; Allocation of Spectrum in the 46.9-47.0 GHz Frequency Band for Wireless Services; and Allocation of Spectrum in the 37.0- 38.0 GHz and 40.0-40.5 GHz for Government Operations*, GN Docket No. 14-77, IB Docket No. 15-256, RM-11664, WT Docket No. 10-112, IB Docket No. 97-95, Report & Order and Further Notice of Proposed Rulemaking, 31 FCC Rcd 8014 (rel. July 14, 2016) (*Spectrum Frontiers Report & Order* or *Spectrum Frontiers Further Notice*).

[3] *Spectrum Frontiers Report & Order*, 31 FCC Rcd at 8106, para. 265.

[4] *See id.* at 8104, para. 262.

new issues raised by 5G security in order to foster dialogue between relevant standards bodies and prospective 5G providers on the best methods for ensuring that networks and devices are secure from the beginning.[5]

4. We are not conducting this NOI in a vacuum. We intend this inquiry to complement the important work on cybersecurity that is already taking place within the government and private sector.[6] The Commission, these other groups, and the wireless industry all have a significant interest in ensuring that these new networks consider security risk and mitigation techniques from the outset. This NOI, and the record it seeks to develop, will help in that effort.

5. We recognize that our inquiry, focusing on cybersecurity for 5G, raises fundamental questions relative to scope and responsibilities. Security of network infrastructure, such as protecting

[5] In issuing this NOI, PSHSB has coordinated with the Office of Engineering and Technology and the Wireless Telecommunications Bureau. *See id.* at 8106, para. 265.

[6] We observe that the U.S. Department of Commerce's National Institute of Standards and Technologies (NIST) NIST recently issued guidelines on cyber security for Internet-connected devices, stressing an engineering-based approach that builds security systems directly into IoT technology. *See* NIST, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure System, NIST Special Pub. 800-160 (Nov. 2016), https://doi.org/10.6028/NIST.SP.800-160. The Department of Homeland Security (DHS) also recently released its own cybersecurity policy for IoT devices, delineating six strategic principles that it believes will help stakeholders stop unauthorized intruders from tampering with connected devices. *See* U.S. Dept. of Homeland Security, Strategic Principles for Securing the Internet of Things (IoT), Version 1.0 (Nov. 15, 2016), https://www.dhs.gov/securingtheIoT. NIST and the National Telecommunications and Information Administration (NTIA) developed a risk management framework for addressing cybersecurity issues. *See* NIST, Framework for Improving Critical Infrastructure Cybersecurity (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf. The Communications Security, Reliability, and Interoperability Council IV's (CSRIC IV's) Cybersecurity Risk Management and Best Practices Working Group 4 developed a segment-specific analysis of the application of the Cybersecurity Framework, as well as recommendations for voluntary efforts to address cybersecurity concerns. *See* CSRIC IV, Working Group 4, Cybersecurity Risk Management and Best Practices, Final Report (2015), https://transition.fcc.gov/pshs/advisory/csric4/CSRIC_IV_WG4_Final_Report_031815.pdf. In addition, the Commission's Technical Advisory Council (The TAC) Cybersecurity Working Group issued its report on applying security to consumer IoT devices on December 4, 2015. *See* Federal Communications Commission Technical Advisory Council (FCC TAC), Cybersecurity Working Group, Technical Considerations White Paper (2015), https://transition.fcc.gov/oet/tac/tacdocs/reports/2015/FCC-TAC-Cyber-IoT-White-Paper-Rel1.1-2015.pdf. *See also* FTC Report on Internet of Things Urges Companies to Adopt Best Practices to Address Consumer Privacy and Security Risks (Jan. 27, 2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf (proposing privacy and cybersecurity best practices associated with IoT); U.S. Dept. of Health and Human Services, Radio Frequency Wireless Technology in Medical Devices: Guidance for Industry and Food and Drug Administration Staff (Aug. 14, 2013), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm077272.pdf (guidance to the industry on considerations for the safe and effective development and use of RF technology in medical devices).

software and hardware that are essential to signaling and control of Radio Access Networks and to ensure the proper operation of the network, creates one perspective. Another perspective, however, just as relevant to the consumer, is the end-to-end security of both the network and the devices that connect to commercial network services. Devices and other network elements may be furnished by the service provider, third parties, and consumers themselves.[7] Who should be responsible for cyber protections for a device, or should responsibility be shared in some recognizable manner across the 5G ecosystem? We also appreciate that 5G is not apt to be a separate network, but rather will be integrated with existing previous generation networks, perhaps indefinitely. Do questions about the cyber protections of 5G networks inherently implicate the other networks associated with them? Where should the lines between networks be drawn relative to responsibility for 5G cybersecurity? We invite comment on these and other questions related to scope in the context of the various specific topics discussed below.

II. INQUIRY

6. This NOI looks holistically at the security implications (*e.g.*, as to IoT) that arise through the provision of a wide variety of services to various market sectors and users in the future 5G network environment.[8] We also explore 5G security threats, solutions, and best practices.[9] By "confidentiality," "integrity," and "availability," or "CIA," we mean those three interrelated, and dynamic principles ("CIA principles") that collectively guide security practices and illustrate the various considerations that must be applied when developing a security posture for communications technologies and services.[10]

---

[7] For example, the same Wi-Fi IoT device may be connected to the Internet using a Mi-Fi hot spot via the carrier's network or via a wireline network such as a cable provider's wireless Wi-Fi router.

[8] We note that this NOI is consistent with, but distinct from, the Commission's privacy rulemaking proceeding. Last month, the Commission released the *Broadband Privacy Order*, which applied the privacy requirements of the Communications Act to broadband service. There, the Commission stated that it expected providers to take CIA principles into account when developing, implementing, and monitoring the effectiveness of adopted measures to meet their data security obligation under Section 222. *See Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, FCC 16-148 at 98, para. 239 (Nov. 2, 2016) (*Broadband Privacy Order*).

[9] As used in this NOI, "security" and "information security" refer to protecting data, networks, and systems from unauthorized access, use, disclosure, disruption, modification, or destruction, in order to protect confidentiality, integrity, and availability with respect to such networks, systems, and defined user communities. *See* 44 U.S.C. § 3552(b)(3). We note this definition of "security" is distinct from the definition of security as it relates to "radios" and radio parameters as defined in 47 CFR § 2.944 or our Part 15 rules. *See*, *e.g.*, 47 CFR § 1.407.

[10] "Confidentiality" refers to protecting data from unauthorized access and disclosure. *See* ATIS, *ATIS Telecom Glossary: Confidentiality* (Aug. 15, 2016), http://www.atis.org/glossary/definition.aspx?id=6609. "Integrity" refers to protecting data from unauthorized modification or destruction, both at rest and in transit. *See* ATIS, *ATIS Telecom Glossary: Integrity* (Aug. 15, 2016), http://www.atis.org/glossary/definition.aspx?id=4584. Finally, "availability" refers to whether a network provides timely, reliable access to data and information services for authorized users. *See* ATIS, *ATIS Telecom Glossary: Availability* (Sept. 7, 2016), http://www.atis.org/glossary/definition.aspx?id=5637. *See also Spectrum Frontiers Report and Order*, 31 FCC Rcd 8106, para. 263 n.672. *See also* Communications Security, Reliability, and Interoperability Council (CSRIC), Working Group 21: Cyber Security Best Practices Final Report at 35 (2011) https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf (utilizing the same definitions of these terms). All three of these principles are fundamental to any security framework and are

(continued….)

7. As an initial matter, we seek to understand the current state of security planning for 5G networks. We must first build a solid foundation of facts about 5G security in order to further identify potential issue areas and solutions. We seek comment on the current efforts across industry to study 5G security, develop security protocols and solutions, and triage 5G security issues when they arise. How are equipment developers considering security in the design of 5G equipment? How are service providers considering security in the planning of 5G networks and ensuring end-to-end security where 5G technology is integrated with prior generation technology in heterogeneous networks? How can the Commission support and enhance this work? What known vulnerabilities require increased study? How should 5G differ in terms of cybersecurity needs from its widely-deployed predecessor generation, 4G LTE? What cybersecurity lessons can be learned from 4G deployment and operational experience that are applicable to the 5G security environment? What should be different, if anything, between LTE pre-5G deployment and post-5G deployment?

8. In this NOI, we seek information on a variety of specific security-related issues. We do not, however, limit our inquiry to these narrow topics. Instead, we encourage commenters to consider this common thread throughout the NOI: how can we, working together with other stakeholders, ensure the rapid deployment of secure 5G networks, services, and technologies?

A. Protecting Confidentiality, Integrity, and Availability

9. As the Commission indicated in the *Spectrum Frontiers Report and Order,* we seek to promote 5G security through a "security-by-design" approach to 5G development,[11] and we believe it is important that *all* stakeholders – service providers, software developers, and device manufacturers alike – work toward a comprehensive long-term strategic framework. We seek comment on the premise that, by utilizing the "confidentiality," "integrity," and "availability" (CIA) principles,[12] a firm may avoid or mitigate 5G network and device data security risk through strong, adaptive, protections against unauthorized use, disclosure, and access. What are the benefits and limitation of a security-by-design approach and of employing CIA principles?

10. We seek specific comment on how the CIA principles are being considered for 5G networks, systems, and devices. In particular, we examine below how CIA principles are being taken into consideration with respect to authentication, encryption, physical security, device security, protecting 5G

(Continued from previous page)

dynamically interrelated, and thus no particular principle should be addressed in isolation if 5G security is to be achieved. *See*, *e.g.*, Techopedia, CIA Triad of Information Security, https://www.techopedia.com/definition/25830/cia-triad-of-information-security (last visited Oct. 5, 2016); *see also* 44 USC § 3552(b) (3) (defining "confidentiality," "integrity," and "availability" (CIA) as the constituent elements of "information security"; collectively, the terms are sometimes referred to as the "CIA principles"); Office of Management and Budget, Circular No. A-130, Managing Information as a Strategic Resource at 36 (2016), https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf (defining "[s]ecurity control" as "the safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information").

[11] *Spectrum Frontiers Report & Order*, 31 FCC at 8106, paras. 255-65.

[12] *See supra* note 10 (further explaining the CIA principles).

networks from cyber attacks, patch management, and risk segmentation of networks. This is a non-exclusive list, and we seek comment on other areas that are potential vulnerabilities for 5G.

1. Authentication

11. Preserving the confidentiality and integrity of networks, systems, and data depends on limiting access to authorized users. This is typically accomplished through effective, and sometimes mutual, authentication.[13] We seek comment on the use of authentication in networks today and whether existing authentication practices will be applicable to the 5G environment. We seek comment on the effective use of mutual authentication, in particular, for protecting 5G networks against unauthorized access and end-user devices against attaching to malicious network components, as well as the perceived limitations and drawbacks of those uses. Are there specific considerations that would apply to 5G devices? Under what circumstances would mutual authentication be considered essential to ensure or bolster security? Are there any circumstances where mutual authentication would not be beneficial? If a communications provider did not invest in mutual authentication, how would that likely affect its relative overall security risk? What other authentications methodologies might be effective for 5G security? Would the mass deployment of high-volume, low-cost 5G devices in IoT networks present particular authentication challenges? How can providers effectively authenticate the communications of high-volume, low-cost 5G devices – device to device, device to network, and network to device? How can providers effectively address these challenges? Would it be appropriate for 5G architects to consider identity credentialing and access management, in addition to authentication?

2. Encryption

12. Encryption can be an important aspect of protecting confidentiality, integrity and availability in communications environments.[14] We seek comment on the planned deployment and use of

[13] Mutual authentication generally requires that both entities involved in a transaction verify each other's identity at the same time. (According to the National Information Assurance Glossary, mutual authentication refers to the process of both entities involved in a transaction verifying each other. *See* Committee on National Security Systems, National Information Assurance (Apr. 26, 2010), https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf. Mutual authentication can be a tool against phishing, replay attacks, and other types of "man-in-the-middle" exploits in communications environments, and is presumably a core security consideration for 5G security. For some communications technology protocols, mutual authentication is established as a default setting; for other protocols, however, it is optional. *See* Secure Shell, *Setting Up Non-Interactive Server and User Authentication*, https://support.ssh.com/manuals/server-zos-eval/54/Setting_up_Non-Interactive_Server_and_User_Authentication.html (last visited Sept. 5, 2016); Tim Dierks & Eric Rescorla, *The Transport Layer Security (TLS) Protocol* (Aug. 2008), https://tools.ietf.org/html/rfc5246. Authentication can be either human to machine, or human to human. Each approach requires forethought, has resource implications, and establishes stakeholder responsibilities.

[14] Encryption is the conversion of electronic data into another form, called "ciphertext", which cannot be easily understood by anyone except authorized parties. *See* Margaret Rouse, *Definition: Ciphertext*, WhatIs.com (2007), http://searchcio-midmarket.techtarget.com/definition/ciphertext (defining "ciphertext"); Margaret Rouse, *Definition: Encryption*, TechTarget (2014), http://searchsecurity.techtarget.com/definition/encryption (defining encryption). Effective encryption is defined as the security of cryptological techniques and related management conducted in accordance with NIST document SP-800-57. *See* Elaine Barker et al., Computer Security at 22 (2012), http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf.

encryption to promote 5G security, as well as on the perceived challenges, costs, and benefits of encryption at both the network and device levels.

13. We seek comment on whether currently available encryption protocols are effective in securing devices and are likely to be effective in a 5G environment in which innumerable, low-cost devices are expected to operate.[15] We seek comment on ways that 5G participants can address encryption key management and distribution mechanism challenges. We additionally seek comment on stakeholder responsibilities with respect to objective encryption key management for 5G.

14. We also seek comment on whether encryption is necessary for all 5G communications. Recent research has shown that certain scenarios exist where signaling information is not encrypted for systems implementing LTE standards, which has led to bad actors being capable of tracking the movements of individuals via their LTE handset.[16] We seek comment on whether the decisions made by the 3GPP standards body that resulted in non-encryption for such systems are rooted in increased latency, degraded performance due to added signaling or computational requirements, an interest in minimizing changes to LTE standards as 5G is standardized, or other factors.[17] We inquire about what lessons, if any, can be learned from the underlying rationale of these decisions as they pertain to encryption for 5G communications.

15. Finally, we seek comment on whether 5G service providers should distinguish between the application of encryption to products that would operate primarily on the 5G control plane and those that would be part of the user plane.[18] If such a distinction is desirable, how should such a distinction be made? For example, if security elements were limited to the control plane, which security elements should be included and what minimum security requirements would apply?

3. Physical Security

16. Physical security aims to protect networks and critical components of end-user devices, even where those devices are in the possession of unauthorized users (lest those devices become operationalized to induce risk to other elements of the 5G ecosystem, downstream users and others). We

[15] The three algorithms used to protect the air interface (handset to tower) are: SNOW 3G, AES, and ZUC. *See* Jeffrey Cichonski & Joshua Franklin, LTE Security – How Good Is It? (Apr. 24, 2015), https://www.rsaconference.com/writable/presentations/file_upload/tech-r03_lte-security-how-good-is-it.pdf.

[16] *See* Roger Piqueras Jover, LTE Security, *Protocol Exploits and Location Tracking Experimentation with Low-Cost Software Radio*, Cornell University Library (Jul. 18, 2016), https://arxiv.org/abs/1607.05171.

[17] *See id*.

[18] There are two core component architectures within the 5G radio protocol architecture stack: the "user plane" and the "control plane." In the user plane, generated data packets are processed by protocols such as TCP, UDP and IP, while in the control plane, the radio resource control (RRC) protocol writes the signaling messages that are exchanged between cellular base stations and mobile devices. In both settings, the information is processed by the packet data convergence protocol (PDCP), the radio link control (RLC) protocol and the medium access control (MAC) protocol, before being passed to the physical layer for transmission. *See LTE Radio Protocol Architecture*, Tutorialspoint, https://www.tutorialspoint.com/lte/lte_radio_protocol_architecture.htm (last visited Nov. 1, 2016); Margaret Rouse, *Definition: Plane (In Networking)*, WhatIs.com, http://whatis.techtarget.com/definition/plane-in-networking (last visited Nov. 1, 2016).

seek comment on physical security objectives and needs in the 5G environment, and on any other considerations the Commission should take into account in its examination of physical security of 5G networks and devices.

17. What device- and network-based physical security methods would be most effective if applied to 5G devices? To what extent does lack of physical security pose a threat to, or introduce risk from unsupervised 5G devices? To what extent does lack of physical security pose a threat to, or introduce risk from unsupervised 5G devices? Will the 5G environment present any new or unique challenges? What other issues and factors should the Commission consider on the question of preserving confidentiality, integrity and availability through physical security?

18. What aspects or uses of 5G networks should be considered "mission critical" (*i.e.*, related to safety) and, as such, do they warrant special consideration with respect to physical security? What "mission critical" activities distinguish these networks and how can they be physically secured in the 5G environment? Should certain 5G networks be physically diverse at the network level as a result of the "mission-critical" aspects they support or enable? If so, how should that diversity be achieved?

4. Device Security

19. Ensuring the provision of confidentiality, integrity, and availability requires that devices are secure and capable of authenticating on the network. What methodologies will be used to protect the variety of devices connected to 5G networks? For example, some devices that will connect to 5G networks will incorporate some form of Subscriber Identity Module (SIM) technology.[19] Is current SIM technology robust enough to ensure security without posing threats to consumers, service providers, or the underlying infrastructure? Will SIM technology be leveraged for 5G? Do standards for next generation SIM cards (*e.g.*, embedded SIMs (eSIMs)) effectively address security and integrity concerns? What new security benefits or challenges are created by the use of eSIMs? Are there non-SIM methods that should be considered for high-volume, low-cost devices, and if so, are standards bodies currently developing standards for such methods? What other issues and factors should the Commission consider on the question of preserving CIA through device security?

5. Protecting 5G Networks from DoS and DDoS Attacks

20. A security exploit that targets network resources, such as a Denial-of-Service (DoS) or Distributed Denial of Service (DDoS) attack, could have an impact on availability of service by causing a total or partial disruption of service.[20] We seek comment and supporting data on the mechanisms most

---

[19] Subscriber Identity Modules (SIMs) are removable components of mobile phones and devices that enable the cell phone to access subscribed services by authenticating the user of the cell phone to the network. SIMs also store personal information, including text messages, contact lists and service-related information. *See* Wayne Jansen & Rick Ayers, *Forensic Software Tools for Cell Phone Subscriber Identity Modules*, National Institute of Standards and Technology, http://csrc.nist.gov/groups/SNS/mobile_security/documents/mobile_forensics/pp-SIM-tools-final.pdf (last visited Nov. 9, 2016).

[20] In a denial-of-service (DoS) attack, an attacker attempts to prevent users from accessing information or services by targeting computers, specific websites or services, or network connections. The most common type of DoS attack occurs when an attacker "floods" a network with information, overloading the server with requests to view a

(continued….)

likely to be effective at preserving confidentiality, integrity and availability through mitigation of DoS and DDoS attack risks in the planned 5G environment, including techniques for protecting both the network control and data planes.[21] Which methods of defense against DoS and DDoS attacks are the most cost-effective?

21. We seek comment on whether additional standards are needed to assist in mitigating DoS and DDoS attacks. Many such attacks involve the forging of IP-sender addresses (spoofing) so the attacking machines cannot be easily identified and to allow amplification of attacks. What anti-spoofing technologies are most likely to be effective in the 5G environment, and what are the challenges to their deployment?

6. Patch Management

22. For more than a decade, communications security authorities and expert bodies, such as the Commission's Federal Advisory Committee for communications security policy development (the Communications Security Reliability and Interoperability Council (CSRIC)), have stressed the importance of regular system patching.[22] Applying security patches and routine patch management can reduce known vulnerabilities in devices and software,[23] reducing the risk of successful security exploits to

(Continued from previous page)

webpage. As a result, the server will be unable to process requests, and a legitimate user will be unable to access the site. *See* United States Computer Emergency Readiness Team, *Security Tip: Understanding Denial of Service Attacks*, https://www.us-cert.gov/ncas/tips/ST04-015 (last visited Nov. 9, 2016). In a distributed denial-of-service (DDoS) attack, an attacker may take control of other users' computers through security vulnerabilities. The attacker can then force the computers to send large amounts of data to a website or email address. The attacker "distributes" these attacks among multiple computers, which work in tandem to overload the server. *See id.*

[21] This may include the use of multiple layers of defense, starting with front-end applications or hardware to block certain types of traffic; key completion indicators; blackholing or sinkholing; intrusion prevention systems; firewalls, routers, and switches; upstream filtering; and DoS defense systems. *See* George Kousiouris, Key Completion Indicators: Minimizing the Effect of DoS Attacks on Elastic Cloud-based Applications Based on Application-level Markov Chain Checkpoints, 622, 623 (2014), https://files.ifi.uzh.ch/stiller/CLOSER%202014/CLOSER/CLOSER/Cloud%20Computing%20Enabling%20Technology/Short%20Papers/CLOSER_2014_118_CR.pdf; *see also* Charalampos Patrikakis et al., *Distributed Denial of Service Attacks*, 7 The Internet Protocol Journal 4 (Dec. 2014), http://www.cisco.com/c/en/us/about/press/internet-protocol-journal/back-issues/table-contents-30/dos-attacks.html; Valter Popeskic, How to Prevent or Stop DoS Attacks? (Oct. 16, 2012), https://howdoesinternetwork.com/2012/prevent-stop-dos-attacks.

[22] *See* Communications Security, Reliability, and Interoperability Council (CSRIC), Working Group 21: Cyber Security Best Practices Final Report at 35 (2011), https://transition.fcc.gov/pshs/docs/csric/WG2A-Cyber-Security-Best-Practices-Final-Report.pdf.

[23] *See*, *e.g.*, *Protect Myself from Cyber Attacks*, Department of Homeland Security (Aug. 8, 2016), https://www.dhs.gov/how-do-i/protect-myself-cyber-attacks ("Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies."); Frontier Communications, *Frontier Communications Encourages Hyper Vigilance When It Comes to Anything Cyber* (Oct. 3, 2013), http://investor.frontier.com/releasedetail.cfm?ReleaseID=794772 ("Keep your operating system, browser, anti-virus and other critical software up to date. Security updates and patches are available for free from major companies."); *Ten Steps to Smartphone Security,* Federal Communications Commission, https://www.fcc.gov/sites/default/files/smartphone_master_document.pdf ("Accept updates and patches to your smartphone's software."), https://www.fcc.gov/sites/default/files/smartphone_master_document.pdf (last visited

(continued….)

devices and networks and enhancing system confidentiality, integrity, and availability. We seek comment and supporting data on patch management's role as part of a service provider's overall security risk management strategy in the 5G environment.[24]

23. We also seek comment on which 5G network elements can be successfully maintained by service providers through patch management. We observe that there are generally four types of patches that are pushed to devices with service provider involvement: (1) patches from service providers to their own infrastructure; (2) patches service providers require and push on to subscriber devices; (3) patches to third-party infrastructure that are leased by service providers but owned by a third party; (4) patches to subscriber devices that are sent by device manufactures under the direction of service providers. For each type of patch, we seek comment on processes that service providers and mobile device manufacturers should adopt to sustain an effective patch management program in the 5G environment. How do service providers and mobile device manufacturers routinely make themselves aware of new vulnerabilities that need to be patched? How soon after a vulnerability is discovered is the corresponding patch pushed to devices? What other mechanisms might preclude unauthenticated code from running on 5G devices that are connected to their networks?

24. We seek comment on how 5G service providers and equipment manufacturers can ensure that critical security software updates are installed on their subscriber devices in a timely fashion. How can 5G service providers effectively ensure firmware and software patch management related to security through their customer relationships?[25] How common is it for manufacturers or service providers to rely on consumers to become aware of and install patches to their software and/or hardware? What do 5G service providers plan to do to help ensure that a subscriber's devices remain "patchable" and/or "discoverable" for purposes of device updates? How can consumers determine whether an older device

(Continued from previous page)

Oct. 24, 2016); *Stop. Think. Connect. Cyber Tips*, Department of Homeland Security (Oct. 15, 2015), http://www.dhs.gov/stopthinkconnect-cyber-tips ("Keep your operating system, browser, and other critical software optimized by installing updates.").

[24] In May 2016, in an effort to better understand, and ultimately to improve, the security of mobile devices, the Commission's Wireless Telecommunications Bureau Chief, Jon Wilkins, sent a letter to six mobile carriers seeking information on their processes for reviewing and releasing security updates for mobile devices. *See* Letter from Jon Wilkins, Chief, Wireless Telecommunications, to Carriers at 1 (May 9, 2016), https://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0509/DOC-339256A2.pdf. At the same time that the Wireless Telecommunications Bureau issued letters to mobile carriers, the FTC issued Section 6(b) Orders to eight mobile device manufacturers requiring them to provide the agency with information on how each manufacturer issues security updates to address vulnerabilities in smartphones, tablets, and other mobile devices. *See* Press Release, FTC, FTC to Study Mobile Device Industry's Security Update Practices (May 9, 2016) https://www.ftc.gov/news-events/press-releases/2016/05/ftc-study-mobile-device-industrys-security-update-practices.

[25] The term "software" is used generally in this context. Many different approaches may be used to store and manage operations configuration of a radio frequency transmitter. These may include configurations based on using Read-only-Memories (ROM), field programmable ROM, firmware used to boot devices, BIOS control, software drivers loaded on system start, sensor based controls, network management systems, external database controls, service provider controls, user interface controls, *etc*.

or service, no longer being sold at retail, is still receiving security-related patches and whether it is still safe to use?

25. Finally, we seek comment on whether relevant standards have been produced that present a common approach, or describe a best practice, to facilitate patch management procedures that can be applied regardless of the underlying device operating system in a 5G ecosystem. In the absence of any deployed standard, should this effort be explored, and if so, which standards body or forum would be the best candidate to address this issue? What other issues and factors should the Commission consider on the question of preserving CIA through patch management?

7. Risk Segmentation

26. Risk segmentation involves splitting network elements into separate components to help isolate security breaches and minimize overall risk. For example, networks can be divided into isolated subnetworks to boost performance and improve security.[26] Risk segmentation or network slicing might allow greater resiliency, more effective cyber threat monitoring and analysis and stronger security for network service supporting critical infrastructure communications (to include ICS and SCADA). We seek comment on the use of segmentation in 5G networks and how segmentation can reduce risk in such networks.

27. We seek comment and supporting data on ways that segmentation could be achieved throughout the 5G ecosystem to ensure service providers have greater situational awareness and ability to respond to, and contain, security threats. What lessons have service providers and other enterprises learned about the application of segmentation in older networks that can be applied to 5G networks? To what extent can service providers use network segmentation technologies, such as a virtual private network (VPN) or other cryptographic separation, to help ensure that no device operating on their network's control plane is directly and immediately accessible via the Internet? Could VPNs or a similar mechanism be scaled in such a way that 5G providers could implement segmentation across their entire ecosystem? We seek comment on the technologies used for network segmentation, and on how to ensure that future networks employing these new architectures use security-by-design principles to minimize security risk.

28. Should segmentation in the 5G environment be based on geography or region, on type of function or device, or by community of interest (such as by public safety, defense, transportation community interests)? To what extent are service providers segmenting physical, logical and virtual risks? We seek comment on what 5G service providers plan to do to establish logical and physical separation of different bands and/or receive antennas in order to improve integrated device security.

29. We seek comment on whether certain network elements or activities merit special consideration with respect to risk segmentation. For example, would it be appropriate to provide virtual separation for Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA),

[26] *See* Nimmy Reichenberg, *Improving Security via Proper Network Segmentation*, SecurityWeek (Mar. 20, 2014), http://www.securityweek.com/improving-security-proper-network-segmentation.

financial, health, and other high-impact, low-risk critical infrastructure functions? To what extent are such segmentation strategies effective in reducing security risk?

30. Risk segmentation can also be applied to devices in terms of firmware, software, and data. In some cases, configuration data (*e.g.*, an Access Class value)[27] may be set as read-only by the device, but can only be changed by the service provider. We seek comment on whether privacy features and requirements have been standardized in organizations like 3GPP (and to what extent they will be standardized for 5G) to support confidentiality and integrity of information. What other issues and factors should we consider on the question of preserving CIA through segmentation?

31. Finally, with respect to each of the topics discussed above, we seek information regarding which standards bodies are involved and the state of standards development to protect CIA in the 5G environment. Is there a need for additional standards body involvement?

B. Additional 5G Security Considerations

1. Overview

32. It is widely expected that 5G networks will be used to connect the myriad devices, sensors and other elements that will form the Internet of Things (IoT). The anticipated diversity and complexity of these networks, how they interconnect, and the sheer number of discrete elements they will comprise raise concerns about the effective management of cyber threats. How can holistic security objectives for 5G be established? What roles can service providers and device manufacturers play to reduce security risk for various communities of interest? How should service providers, device manufacturers, standards bodies and the Commission coordinate their efforts? Are there particular standards being developed for 5G IoT applications? Finally, we seek comment on benefits and costs associated with effective hardware, firmware, software, and application security for 5G.

33. We generally seek comment on the extent to which IoT devices could place 5G networks at unique risk. For example, are there particular vulnerabilities that arise from, or are increased by, the fact that 5G communications have relatively short range and rely on multiple access points? It is possible that some of IoT devices will have limited security features. Others may be deployed in locations where regular monitoring is not possible. Could this have a negative effect on overall 5G network security? If so, what roles can network equipment providers, ISPs and device manufacturers play, by themselves and in coordination, to mitigate the risks? Are any lessons being learned from the October 2016 DDoS attacks relevant to 5G?[28] Where risk externalities exist? How will the 5G marketplace address cybersecurity risk in the commons?

---

[27] The Access Class is a value between 0 and 16 that can be used to prioritize a handset's ability to establish a connection with the network. Conceptually, the higher the value, the higher the probability of establishing the connection. A successful connection would provide dial tone to the user.

[28] *See* Nicole Perlroth, Hackers Used New Weapons to Disrupt Major Websites Across U.S., The New York Times (Oct. 21, 2016), http://www.nytimes.com/2016/10/22/business/internet-problems-attack.html.

34. We also seek comment on whether and how security needs for 5G IoT devices might differ from other infrastructures, including, in particular, each of the critical infrastructure sectors. What expectations would various critical infrastructure sectors likely have for the security capabilities and features of 5G services? Does the government have a role where residual risk unduly threatens critical infrastructure or national security, and if so, what should it be?

35. Given the likely unprecedented diversity of connected devices and their manufacturers, we also generally seek comment on whether 5G security could be challenged by hardware issues, including threats from a compromised supply chain. How are service providers and equipment manufacturers currently assessing supply chain risks? Are they assessing risks consistent with NIST guidelines?[29] We seek comment on whether, and if so, how 5G service providers should ensure the provenance of the hardware, firmware, software, and applications operating in their environments. What special considerations, if any, should be applied relative to 5G supply chain risks?

36. We further seek comment on benefits and costs associated with effective hardware, firmware, software, and application security for 5G. What are the costs associated with updating existing hardware, firmware, software, and applications versus the costs of adding entirely new elements for a totally new security posture? Is there a role for 5G-specific third party security entities? Do benefits and costs vary depending on the use of open-source software compared to proprietary software? What are the costs of adding security-specific features to 5G network hardware, firmware, software and applications? Are there scale economies observed across local, regional, and nationwide 5G networks? Finally, what other issues or factors should the Commission consider with respect to the preservation of confidentiality, integrity and availability in the 5G environment?

2. Roles and Responsibilities

37. Because of the anticipated proliferation of 5G networks and the devices that will be deployed on them, there is a chance that the cyber integrity of the network as a whole could be overlooked on the assumption that another network participant would be responsible. Is this a valid concern? We seek general comment on who should be responsible for assuring cyber security across the 5G ecosystem, what principles should guide the management of cyber risk, and how cyber risk should be

[29] NIST, in a series of publications, addresses the subject of supply chain risk management (SCRM) issues. They include: NIST Special Publication 800-30, Revision 1, *Guide for Conducting Risk Assessments*, to integrate SCRM into the risk assessment process (NIST SP 800-30 Rev. 1); NIST Special Publication 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (NIST SP 800-37 Rev. 1); NIST Special Publication 800-39, *Managing Information Security Risk: Organization, Mission, and. Information System View*, helping to integrate SCRM into the risk management tiers and risk management process (NIST SP 800-39); NIST 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, providing guidance on information security controls for enhancing and tailoring to the SCRM context (NIST SP 800-53 Rev. 4); NIST Special Publication 800-53A Revision 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, Building Effective Security Assessment Plans*, which enables the assessment techniques applicable to SCRM controls (NIST SP 800-53A Rev. 4); and NIST Special Publication 800-161, which refines the multi-tiered risk management approach of NIST SP 800-39 by providing SCRM guidance at the Organization, Mission, and Information System Tiers, and also contains an enhanced overlay of special SCRM controls, building on NIST SP 800-53 Rev. 4.

managed within companies. How should providers work together across the 5G ecosystem to achieve desirable outcomes in cyber risk management?

38. Relatedly, we seek information on how the 5G ecosystem will share information about cyber threats and concerns. For example, Information Sharing and Analysis Organizations (ISAO) standards are still largely a work in progress, and their success depends on the level of industry participation. We seek comment on whether an ISAO construct could be or should be applied to the 5G ecosystem. Would it be appropriate to develop a 5G-specific ISAO? Should 5G networks be instrumented to support automated cybersecurity threat indicators and network anomaly information sharing and analysis? Is an ISAO or multiple ISAOs the right focal point for automated cyber information sharing and analysis? Should it address IoT concerns more broadly or focus on network-based considerations? Who should be involved? Should work of ISAOs dealing with related topics be formally coordinated? If so, how? What are the proper roles of standards bodies, advisory committees such as the North American Numbering Council (NANC), industry authorities, numbering and data services and the FCC?

39. We observe that the NIST Framework for Improving Critical Infrastructure Cybersecurity Framework (NIST CSF)[30] has been voluntarily used by members of the critical infrastructure community, including the communications sector, for several years to help manage cybersecurity risk. We seek comment on whether, and if so how, the NIST CSF can be used to manage risk for 5G service providers and networks. We note, in particular, that the NIST CSF includes several top level organizational functions that can be performed concurrently and continuously to form an operational culture that addresses dynamic security risk, namely, Identify, Detect, Protect, Respond, and Recover (IPDRR).[31] We seek comment on unique factors with respect to these functions that should guide 5G design, standards development and operations.

3. Other Considerations

40. Are there additional functions that should be considered in the 5G environment? How should addressing and naming be accommodated for 5G?[32] Are stakeholders working to evolve any of

---

[30] National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cyberframework (last visited Nov. 8, 2016); Press Release, Office of the Press Secretary, Statement by the President on the Report of the Commission on Enhancing National Cybersecurity (Dec. 2, 2016), https://www.whitehouse.gov/the-press-office/2016/12/02/statement-president-report-commission-enhancing-national-cybersecurity (supporting the recommendation of the nonpartisan Commission on Enhancing National Cybersecurity to expand the use of the NIST CSF "in the Federal government, the private sector, and abroad"). *See generally* National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[31] National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity* at 8-9 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

[32] *See* Broadband Internet Technical Advisory Group (BITAG), Internet of Things (IoT) Security and Privacy Recommendations: A Broadband Internet Technical Advisory Group Technical Working Group Report at 22 (2016), https://www.bitag.org/documents/BITAG_Report_-_Internet_of_Things_(IoT)_Security_and_Privacy_Recommendations.pdf (BITAG Report). The BITAG Report

(continued….)

today's numbering schemas to encompass 5G? What practical steps should 5G planners take in order to ensure that the functions discussed in this NOI, and any other relevant functions, are properly considered and implemented within their respective organizations?

4. Benefits and Costs

41. We seek comment on the public harm expected to result from failure to integrate confidentiality, integrity and availability into 5G networks through authentication, encryption, physical and device security, protecting against DoS attacks, patch management and risk segmentation. Could failure to implement these measures decrease broadband adoption and detract from its productive economic use? Could it reduce the risk of loss of competitively sensitive information for businesses? Could it prevent the loss of consumers' personally identifiable information? Could it play a role in preventing the unnecessary loss of life or property by, for example, preventing malicious intrusion into critical infrastructure? How should we quantify these benefits in terms of their economic impact? What other benefits would likely stem from an appropriately secure 5G network?

42. We also seek comment on the costs associated with the implementation of the measures discussed above as investments early in the design and build plans of networks, as opposed to "bolt-on" security after deployment. Are there opportunities for 5G implementation that would only be realized if networks are perceived to be secure? Are there some security elements that, by plan, should be "just in time" or reactive investments, based on realized threats, after 5G implementation? Would these costs include those associated with updating existing hardware, firmware, software, and applications? How would the costs of system updates compare to the costs of adding entirely new elements for a totally new security posture? Do benefits and costs vary depending on the use of open-source software compared to proprietary software? If so, to what extent are open-source solutions available that could reduce costs? Are there scale economies observed across local, regional and nationwide 5G networks? We seek comment on specific costs associated with authentication, encryption, physical and device security, protecting against DDoS attacks, patch management and risk segmentation in the 5G environment.

C. 5G Implications for Public Safety

43. Many public safety services and technologies are undergoing radical change as underlying networks transition from legacy to IP-based modes. Examples include the transition of the nation's 911 system to Next Generation 911 (NG911); the evolution of first responder communications from land mobile radio (LMR) to LTE, including the development of FirstNet; and the emergence of enhanced emergency alerting services that rely on IP-based technologies to communicate with the public. Will any new categories of public safety sensors or other machine-based tools become an included part of 5G public safety communications architecture? We anticipate that the development of 5G networks will contribute new capabilities to these IP-based public safety platforms while also creating new challenges, including security challenges, for public safety entities.

(Continued from previous page)

maintains that IoT devices should support recent best practices for IP addressing and the use of the Domain Name System, and support the most recent version of the Internet Protocol, IPv6.

44. We seek comment on the security implications of linking or integrating 5G networks with IP-based public safety communications platforms. Could this create new security risks or vulnerabilities for NG911, first responder communications, or emergency alerting? What responsibility should 5G service providers have for mitigating and managing these risks? Conversely, could 5G networks help *reduce* security risks that public safety faces in migrating from legacy to IP-based technologies? For example, first responders are planning to make use of Identity Credential, and Access Management (ICAM) services to enable fast and reliable access to various emergency networks, applications, and databases during times of crisis.[33] Effective implementation of ICAM will be especially important for responding to large-scale emergencies that span jurisdictional boundaries because without a secure access management protocol, inter-jurisdictional communication and access to critical information and applications may be compromised. Could 5G services support ICAM in a manner that reduces these security risks? Should public safety anticipate a need for unmanned, unattended device ICAM? Are there special considerations for standards development for public safety services and technologies for 5G, and if so, are standards bodies addressing these issues? Is there a need for additional standards body involvement?

III. PROCEDURAL MATTERS

A. *Ex Parte* Rules

45. This proceeding shall be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[34] Persons making *ex parte* presentations must file a copy of any written presentation or a memorandum summarizing any oral presentation within two business days after the presentation (unless a different deadline applicable to the Sunshine period applies). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentation must (1) list all persons attending or otherwise participating in the meeting at which the *ex parte* presentation was made, and (2) summarize all data presented and arguments made during the presentation. If the presentation consisted in whole or in part of the presentation of data or arguments already reflected in the presenter's written comments, memoranda or other filings in the proceeding, the presenter may provide citations to such data or arguments in his or her prior comments, memoranda, or other filings (specifying the relevant page and/or paragraph numbers where such data or arguments can be found) in lieu of summarizing them in the memorandum. Documents shown or given to Commission staff during *ex parte* meetings are deemed to be written *ex parte* presentations and must be filed consistent with rule 1.1206(b). In

[33] Public safety professionals need immediate access to critical information from the wide variety of systems technology available (*e.g.*, portable computers, tablets and smartphones) to make the best possible decisions and protect themselves and the public. Work continues to be done with the purpose of resolving these access and security issues, often referred to as Identity, Credential, and Access Management (ICAM). *See* First Responder Network Authority, http://www.firstnet.gov/newsroom/blog/psac-completes-icam-and-local-control-task-teams (last visited Oct. 19, 2016). Several public safety network initiatives, such as FirstNet and NENA's NG911 project, continue to work towards an interoperable ICAM solution for next generation public safety networks. *See generally* Identity, Credential, and Access Management, Recommended Principles and Actions Report (2015), https://www.ise.gov/sites/default/files/ICAM_Summit_Report.pdf.

[34] 47 CFR § 1.1200 *et seq.*

proceedings governed by rule 1.49(f) or for which the Commission has made available a method of electronic filing, written *ex parte* presentations and memoranda summarizing oral *ex parte* presentations, and all attachments thereto, must be filed through the electronic comment filing system available for that proceeding, and must be filed in their native format (*e.g.*, .doc, .xml, .ppt, searchable .pdf). Participants in this proceeding should familiarize themselves with the Commission's *ex parte* rules.

B. Comment Period and Procedures

46. Pursuant to sections 1.415 and 1.419 of the Commission's rules, 47 CFR §§ 1.415, 1.419, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using the Commission's Electronic Comment Filing System (ECFS). *See Electronic Filing of Documents in Rulemaking Proceedings*, 63 FR 24121 (1998).

- Electronic Filers: Comments may be filed electronically using the Internet by accessing the ECFS: http://fjallfoss.fcc.gov/ecfs2/.

- Paper Filers: Parties who choose to file by paper must file an original and one copy of each filing. If more than one docket or rulemaking number appears in the caption of this proceeding, filers must submit two additional copies for each additional docket or rulemaking number.

  Filings can be sent by hand or messenger delivery, by commercial overnight courier, or by first-class or overnight U.S. Postal Service mail. All filings must be addressed to the Commission's Secretary, Office of the Secretary, Federal Communications Commission.

  - All hand-delivered or messenger-delivered paper filings for the Commission's Secretary must be delivered to FCC Headquarters at 445 12th St., SW, Room TW-A325, Washington, DC 20554. The filing hours are 8:00 a.m. to 7:00 p.m. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes and boxes must be disposed of before entering the building.

  - Commercial overnight mail (other than U.S. Postal Service Express Mail and Priority Mail) must be sent to 9300 East Hampton Drive, Capitol Heights, MD 20743.

  - U.S. Postal Service first-class, Express, and Priority mail must be addressed to 445 12th Street, SW, Washington DC 20554.

C. Accessible Formats

47. To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an email to fcc504@fcc.gov or call the Consumer & Governmental Affairs Bureau at 202-418-0530 (voice), 202-418-0432 (tty).

D. Further Information

48. For further information, contact Gregory Intoccia of the Public Safety and Homeland Security Bureau, Communications Cybersecurity and Reliability Division, at (202) 418-0546 or at Gregory.Intoccia@fcc.gov.

IV. ORDERING CLAUSES

49. Accordingly, **IT IS ORDERED,** pursuant to the authority contained in Sections 1, 4(i) & (j), 303(r), and 403 of the Communications Act of 1934, 47 U.S.C. §§ 154(i) & (j), 303(r), and 403, that this *Notice of Inquiry* **IS ADOPTED.**

FEDERAL COMMUNICATIONS COMMISSION

David Grey Simpson
Rear Admiral, USN (ret.)
Chief, Public Safety & Homeland Security Bureau