ACTION: Notice.

SUMMARY: The Environmental Protection Agency is planning to submit an information collection request (ICR), ''National Estuary Program (Renewal)'' (EPA ICR No. 1500.08, OMB Control No. 2040–0138) to the Office of Management and Budget (OMB) for review and approval in accordance with the Paperwork Reduction Act. Before doing so, EPA is soliciting public comments on specific aspects of the proposed information collection as described below. This is a proposed extension of the ICR, which is currently approved through June 30, 2017. An Agency may not conduct or sponsor and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number.

DATES: Comments must be submitted on or before March 24, 2017.

ADDRESSES: Submit your comments, referencing Docket ID No. EPA–HQ–OW–2006–0369, online using *www.regulations.gov* (our preferred method), by email to *OW-Docket@epa.gov,* or by mail to: EPA Docket Center, Environmental Protection Agency, Mail Code 28221T, 1200 Pennsylvania Ave. NW., Washington, DC 20460.

EPA's policy is that all comments received will be included in the public docket without change including any personal information provided, unless the comment includes profanity, threats, information claimed to be Confidential Business Information (CBI) or other information whose disclosure is restricted by statute.

FOR FURTHER INFORMATION CONTACT: Vince Bacalan, Oceans and Coastal Protection Division, Office of Wetlands, Oceans, and Watersheds, (Mail Code 4504T), Environmental Protection Agency, 1200 Pennsylvania Ave. NW., Washington, DC 20460; telephone number: 202–566–0930; fax number: 202–566–1336; email address: *bacalan.vince@epa.gov.*

SUPPLEMENTARY INFORMATION: Supporting documents which explain in detail the information that the EPA will be collecting are available in the public docket for this ICR. The docket can be viewed online at *www.regulations.gov* or in person at the EPA Docket Center, WJC West, Room 3334, 1301 Constitution Ave. NW., Washington, DC. The telephone number for the Docket Center is 202–566–1744. For additional information about EPA's public docket, visit *http://www.epa.gov/dockets.*

Pursuant to section 3506(c)(2)(A) of the PRA, EPA is soliciting comments and information to enable it to: (i) Evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the Agency, including whether the information will have practical utility; (ii) evaluate the accuracy of the Agency's estimate of the burden of the proposed collection of information, including the validity of the methodology and assumptions used; (iii) enhance the quality, utility, and clarity of the information to be collected; and (iv) minimize the burden of the collection of information on those who are to respond, including through the use of appropriate automated electronic, mechanical, or other technological collection techniques or other forms of information technology, *e.g.,* permitting electronic submission of responses. EPA will consider the comments received and amend the ICR as appropriate. The final ICR package will then be submitted to OMB for review and approval. At that time, EPA will issue another **Federal Register** notice to announce the submission of the ICR to OMB and the opportunity to submit additional comments to OMB.

Abstract: The National Estuary Program (NEP) involves collecting information from the state or local agency or nongovernmental organizations that receive funds under Sec. 320 of the Clean Water Act (CWA). The regulation requiring this information is found at 40 CFR part 35.

Prospective grant recipients seek funding to develop or oversee and coordinate implementation of Comprehensive Conservation Management Plans (CCMPs) for estuaries of national significance. In order to receive funds, grantees must submit an annual workplan to EPA which are used to track performance of each of the 28 estuary programs currently in the NEP. EPA provides funding to NEPs to support long-term implementation of CCMPs if such programs pass a program evaluation process. The primary purpose of the program evaluation process is to help EPA determine whether the 28 programs included in the National Estuary Program (NEP) are making adequate progress implementing their CCMPs and therefore merit continued funding under Sec. 320 of the Clean Water Act. EPA also requests that each of the 28 NEPs receiving Sec. 320 funds report information that can be used in the GPRA reporting process. This reporting is done on an annual basis and is used to show environmental results that are being achieved within the overall National Estuary Program. This information is ultimately submitted to Congress along with GPRA information from other EPA programs.

Form Numbers: None.

Respondents/affected entities: Entities potentially affected by this action are those state or local agencies or nongovernmental organizations in the National Estuary Program (NEP) who receive grants under Section 320 of the Clean Water Act.

Respondent's obligation to respond: Required to obtain or retain a benefit (Section 320 of the Clean Water Act).

Estimated number of respondents: 28 (total).

Frequency of response: Annual.

Total estimated burden: 5,460 hours (per year). Burden is defined at 5 CFR 1320.03(b).

Total estimated cost: $247,338 (per year), includes $0 annualized capital or operation & maintenance costs.

Changes in Estimates: There will likely be an increase in the total estimated respondent burden compared with the ICR currently approved by OMB. This increase is due to program evaluations taking place in the next three years, compared to only two years in the currently approved ICR. Note that these numbers will be updated in the final FR Notice.

Dated: January 12, 2017.

Marcus Zobrist,

Acting Director, Oceans and Coastal Protection Division.

[FR Doc. 2017–01422 Filed 1–19–17; 8:45 am]

BILLING CODE 6560–50–P

FEDERAL COMMUNICATIONS COMMISSION

[PS Docket No. 16–353; DA16–1282]

Fifth Generation Wireless Network and Device Security

AGENCY: Federal Communications Commission.

ACTION: Notice.

SUMMARY: In this document, the Commission seeks comment on new security issues that implementation of the fifth generation (5G) wireless network and device security presents to the general public, and on the current state of planning to address these issues. The inquiry, focusing on cybersecurity for 5G, raises fundamental questions about scope and responsibilities for such security. The goal of this proceeding is to begin a conversation on the state of 5G wireless network and device security and to foster a dialogue on the best methods for ensuring that the 5G wireless networks and devices used by service providers in their

operations are secure from the beginning.

DATES: Comments are due on or before April 24, 2017; reply comments are due on or before May 23, 2017.

ADDRESSES: You may submit comments, identified by PS Docket No. 16–353, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions comments.
- *Federal Communications Commission's Web site: http://fjallfoss.fcc.gov/ecfs2/.* Follow the instructions for submitting comments.
- *Mail:* 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.
- *People with Disabilities:* Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, etc.) by email: *FCC504@fcc.gov* or phone: (202) 418–0530 or TTY: (202) 418–0432.

For detailed instructions for submitting comments and additional information on the rulemaking process, see the **SUPPLEMENTARY INFORMATION** section of this document.

FOR FURTHER INFORMATION CONTACT: For further information, contact Gregory Intoccia of the Public Safety and Homeland Security Bureau, Communications Cybersecurity and Reliability Division, at (202) 418–1470 or at *Gregory.Intoccia@fcc.gov.*

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's *Notice of Inquiry,* DA 16–1282, adopted and released on December 16, 2016. The full text is available for public inspection and copying during regular business hours in the FCC Reference Center, Federal Communications Commission, 445 12th Street SW., Room CY–A257, Washington, DC 20554. This document will also be available via ECFS at *http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db1216/DA-16-1282A1.pdf.* Documents will be available electronically in ASCII, Microsoft Word, and/or Adobe Acrobat. The complete text may be purchased from the Commission's copy contractor, 445 12th Street SW., Roomy CY–B402, Washington, DC 20554. Alternative formats are available for people with disabilities (Braille, large print, electronic files, audio format), by sending an email to *fcc504@fcc.gov* or calling the Commission's Consumer and Governmental Affairs Bureau at (202) 418–0530 (voice), (202) 481–0432 (TTY).

Synopsis

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.

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. The Federal Communications Commission (FCC) has an opportunity at this stage to ensure that these new technologies and networks are secure by design. Therefore, while the FCC is moving quickly to make the spectrum needed for 5G available in the near term, 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 FCC reiterated its view that communications providers are generally in the best position to evaluate and address security risks to network operations. Toward this end, the FCC 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. The Public Safety and Homeland Security Bureau (PSHSB) issues this Notice of Inquiry (NOI) to seek input on the 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.

4. PSHSB intends this inquiry to complement the important work on cybersecurity that is already taking place within the government and private sector. The FCC, 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. PSHSB recognizes that the inquiry, focusing on cybersecurity for 5G, raises fundamental questions relative to scope and responsibilities. Security of network infrastructure, such as protecting 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, 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. Who should be responsible for cyber protections for a device, or should responsibility be shared in some recognizable manner across the 5G ecosystem? PSHSB also appreciates 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?

II. Inquiry

6. This NOI looks holistically at the security implications arising through the provision of a wide variety of services to various market sectors and users in the future 5G network environment. The NOI also explores 5G security threats, solutions, and best practices. 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. The terms ''confidentiality,'' ''integrity,'' and ''availability,'' or ''CIA,'' are meant to refer to those three interrelated, and dynamic 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. Confidentiality'' refers to protecting data from unauthorized access and

disclosure. ''Integrity'' refers to protecting data from unauthorized modification or destruction, both at rest and in transit. Finally, ''availability'' refers to whether a network provides timely, reliable access to data and information services for authorized users. All three of these principles are fundamental to any security framework and are dynamically interrelated, and thus no particular principle should be addressed in isolation if 5G security is to be achieved.

7. As an initial matter, the NOI seeks to understand the current state of security planning for 5G networks. Please 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 FCC 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. The Commission encourages commenters to consider this common thread throughout the NOI: how can the FCC, working together with other stakeholders, ensure the rapid deployment of secure 5G networks, services, and technologies?

A. Protecting Confidentiality, Integrity, and Availability

9. The FCC seeks to promote 5G security through a ''security-by-design'' approach to 5G development. The NOI seeks comment on the premise that, by utilizing the ''confidentiality,'' ''integrity,'' and ''availability'' (CIA) principles, 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. Please comment on how the CIA principles are being considered for 5G networks, systems, and devices. In particular, the NOI examines below how CIA principles are being taken into consideration with respect to authentication, encryption, physical security, device security, protecting 5G networks from cyber attacks, patch management, and risk segmentation of networks. This is a non-exclusive list, and comment is requested 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. Mutual authentication generally requires that both entities involved in a transaction verify each other's identity at the same time. The NOI seeks comment on the use of authentication in networks today and whether existing authentication practices will be applicable to the 5G environment. The NOI further seeks 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. The NOI seeks comment on the planned deployment and use of 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. Please 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, as well as ways that 5G participants can address encryption key management and distribution mechanism challenges. Additionally comment is requested on stakeholder responsibilities with respect to objective encryption key management for 5G.

14. Please also comment on whether encryption is necessary for all 5G communications, and whether the decisions made by the 3rd Generation Partnership Project (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. Please comment on what lessons, if any, can be learned from the underlying rationale of these decisions as they pertain to encryption for 5G communications.

15. Finally, the NOI seeks 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. If such a distinction is desirable, how should such a distinction be made?

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. Please comment on physical security objectives and needs in the 5G environment, and on any other considerations the FCC 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 FCC 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'' 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? 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 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 FCC 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. The NOI seeks comment and supporting data on the mechanisms most 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. Which methods of defense against DoS and DDoS attacks are the most cost-effective?

21. Please comment on whether additional standards are needed to assist in mitigating DoS and DDoS 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 FCC's Federal Advisory Committee for communications security policy development The FCC seeks 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.

23. Please also comment on which 5G network elements can be successfully maintained by service providers through patch management. 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, please 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. Please 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? 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 or service, no longer being sold at retail, is still receiving security-related patches and whether it is still safe to use?

25. Finally, please 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 FCC 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. 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). Please comment on the use of segmentation in 5G networks and how segmentation can reduce risk in such networks.

27. Please provide comments 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? Please 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? To what extent are service providers segmenting physical, logical and virtual risks? Please 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. Please comment on whether certain network elements or activities merit special consideration with respect to risk segmentation. 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 may be set as read-only by the device, but can only be changed by the service provider. Please 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 the FCC consider on the question of preserving CIA through segmentation?

31. Finally, with respect to each of the topics discussed above, the FCC seeks 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 FCC coordinate their efforts? Are there particular standards being developed for 5G IoT applications? Finally, please comment on benefits and costs associated with effective hardware, firmware, software, and application security for 5G.

33. Please provide comments 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. 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? Where risk externalities exist? How will the 5G marketplace address cybersecurity risk in the commons?

34. Please 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, comment is sought 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? The FCC seeks 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. Please 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 FCC 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? Please provide comments 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 managed within companies. How should providers work together across the 5G ecosystem to achieve desirable outcomes in cyber risk management?

38. Relatedly, please provide information on how the 5G ecosystem will share information about cyber threats and concerns. Please comment on whether an Information Sharing and Analysis Organization (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. The NIST Framework for Improving Critical Infrastructure Cybersecurity Framework (NIST CSF) has been voluntarily used by members of the critical infrastructure community, including the communications sector, for several years to help manage cybersecurity risk. Please comment on whether, and if so how, the NIST CSF can be used to manage risk for 5G service providers and networks. 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). Please 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? Are stakeholders working to evolve any of 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. Please 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 the FCC quantify these benefits in terms of their economic impact? What other benefits would likely stem from an appropriately secure 5G network?

42. Please 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? Please 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. Will any new categories of public safety sensors or other machine-based tools become an included part of 5G public safety communications architecture? The development of 5G networks will potentially contribute new capabilities to these IP-based public safety platforms while also creating new challenges, including security challenges, for public safety entities.

44. Please 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? 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. 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 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.

Federal Communications Commission.

David Grey Simpson,

Chief, Public Safety & Homeland Security Bureau.

[FR Doc. 2017–01325 Filed 1–19–17; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL DEPOSIT INSURANCE CORPORATION

Sunshine Act Meeting

Pursuant to the provisions of the ''Government in the Sunshine Act'' (5 U.S.C. 552b), notice is hereby given that at 10:01 a.m. on Wednesday, January 18, 2017, the Board of Directors of the Federal Deposit Insurance Corporation met in closed session to consider matters related to the Corporation's supervision, corporate, and resolution activities.

In calling the meeting, the Board determined, on motion of Vice Chairman Thomas M. Hoenig, seconded by Director Thomas J. Curry (Comptroller of the Currency), concurred in by Director Richard Cordray (Director, Consumer Financial Protection Bureau), and Chairman Martin J. Gruenberg, that Corporation business required its consideration of the matters which were to be the subject of this meeting on less than seven days' notice to the public; that no earlier notice of the meeting was practicable; that the public interest did not require consideration of the matters in a meeting open to public observation; and that the matters could be considered in a closed meeting by authority of