of the person submitting the application or nomination.

If, in response to this notice, representatives of additional interest groups request membership or representation in the negotiating group, HRSA will determine whether that representative should be added to the NR Committee or simply asked to submit its comments and concerns to us and to another Committee member. HRSA will make that decision based on whether the interest group:

- Would be significantly affected by the rule; and
- Is or is not already adequately represented on the proposed NR Committee.

D. Establishing the Committee

After reviewing any public comments on this Notice and any requests for additional representation, HRSA will take the final steps required to form the Committee.

VI. Negotiation Procedures

If and when this NR Committee is formed, the following procedures and guidelines will apply, unless they are modified as a result of comments received on this notice or during the negotiating process.

A. Facilitator

HRSA will use a neutral facilitator. The facilitator will not be involved with advocating for substantive aspects of the regulation. The facilitator's role is to:

- Chair negotiating sessions, assuring equal opportunity among the various members to present their points of view;
- Help the negotiation process to run smoothly; and
- Help participants define and reach consensus.

B. Good Faith Negotiations

Participants must be willing to negotiate in good faith, and must be authorized to so negotiate by the leaders of the organizations/groups/interests they represent. This may best be accomplished by the selection of senior officials of the affected organizations or groups as participants, and/or by the selection of experienced individuals in such organizations/groups who have expertise in the issues subsumed by this rule and who have access to such senior officials, allowing them to obtain concurrence at each stage of the NR process. This applies to HRSA as well, and HRSA will appoint an appropriate representative, to represent HRSA/HHS when the committee is appointed. (Representatives of components of HRSA and CMS which use the MUP and HPSA designations will also be invited to attend the NR meetings as resources on how their programs relate to the designations, but the HRSA/HHS representative will be the spokesperson for HRSA and HHS interests in this NR effort and will meet with other HHS component representatives between NR Committee meetings to maximize coordination.)

C. Administrative Support

HRSA will supply logistical, administrative and management support. HRSA will also provide technical support to the Committee in gathering and analyzing appropriate indicator data, methodologies and other information relevant to the Committee's work, and conduct appropriate impact analyses, with contractual support from John Snow, Inc. (JSI).

D. Meetings

Meetings will typically be held in the DC metropolitan area or, if necessary, in another location, at the convenience of the Committee. HRSA will announce scheduled Committee meetings and agendas either in the **Federal Register** or on a committee Web site, yet to be established, whose location will be published in the **Federal Register**. Unless announced otherwise, meetings are open to the public.

E. Committee Procedures

Under the general guidance and direction of the facilitator, and subject to any applicable legal requirements, the members will establish at the first meeting the detailed procedures for committee meetings which they consider most appropriate.

F. Defining Consensus

The goal of the negotiating process is consensus. Under the Negotiated Rulemaking Act, consensus generally means that each interest group represented concurs in the result, unless the term is defined otherwise by the Committee. HRSA expects the participants to agree upon their working definition of this term at the first meeting.

G. Failure of Advisory Committee to Reach Consensus

Parties to the NR effort may withdraw at any time. If this happens, the remaining Committee members and HRSA will evaluate whether the Committee should continue.

If the Committee is unable to reach consensus, HRSA will proceed to develop a proposed/interim final rule on its own, as described above.

H. Record of Meetings

In accordance with FACA's requirements, minutes of all Committee meetings will be kept. The minutes will be placed on the Committee's Web site and a copy kept in the public rulemaking record.

Dated: May 6, 2010.

Mary Wakefield,

Administrator, Health Resources and Services Administration.

Dated: May 6, 2010.

Kathleen Sebelius,

Secretary.

[FR Doc. 2010–11214 Filed 5–7–10; 11:15 am]

BILLING CODE 4165–15–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Chapter I

[PS Docket No. 10–93; FCC 10–63]

Cyber Security Certification Program

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: This document seeks comment on whether the Commission should establish a voluntary program under which participating communications service providers would be certified by the FCC or a yet to be determined third party entity for their adherence to a set of cyber security objectives and/or practices. The Commission also seeks comment on other actions it should take, if any, to improve cyber security and to improve education on cyber security issues. The Commission's goals in this proceeding are to increase the security of the nation's broadband infrastructure, promote a culture of more vigilant cyber security among participants in the market for communications services, and offer end users more complete information about their communication service providers' cyber security practices.

DATES: Comments are due on or before July 12, 2010 and reply comments are due on or before September 8, 2010.

ADDRESSES: You many submit comments, identified by PS Docket No. 10–93 and/or rulemaking FCC 10–63, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.
- *Federal Communications Commission's Web Site: http://fjallfoss.fcc.gov/ecfs2/.* Follow the instructions for submitting comments.

• *Mail:* Parties who choose to file by paper can submit filings 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. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes 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. Parties who choose to file by paper must file an original and four copies of each filing. Include docket number PS Docket No. 10–93 and/or rulemaking FCC 10–63 in the subject line of the message.

• *People with disabilities:* Contact the FCC to request reasonable accommodations (accessible format documents, sign language interpreters, CART, *etc.*) by e-mail: *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: Jeffery Goldthorp, Chief, Communications Systems Analysis Division, Public Safety and Homeland Security Bureau, at 202–418–1096.

SUPPLEMENTARY INFORMATION: This is a summary of the Commission's Notice of Inquiry (NOI) in PS Docket No. 10–93, FCC 10–63, adopted and released on April 21, 2010. The complete text of this document is available for inspection and copying during normal business hours in the FCC Reference Information Center, Portals II, 445 12th Street, SW., Room CY–A257, Washington, DC 20554. It is also available on the Commission's Web site at *http://www.fcc.gov/headlines.html.* This document may also be purchased from the Commission's duplicating contractor Best Copy and Printing, Inc., Portals II, 445 12th Street, SW., Room CY–B402, Washington, DC 20554, telephone (800) 378–3160 or (202) 488–5300, facsimile (202) 488–5563, or via e-mail at *fcc@bcpiweb.com.* To request materials in accessible formats for people with disabilities (braille, large print, electronic files, audio format), send an e-mail to *fcc504@fcc.gov* or call the Consumer & Governmental Affairs Bureau at 202–418–0530 (voice), 202–418–0432 (tty).

Summary of the Notice of Inquiry

Background

This NOI seeks comment on whether the Commission should establish a voluntary program under which participating communications service providers would be certified by the FCC or a yet to be determined third party entity for their adherence to a set of cyber security objectives and/or practices. The Commission seeks comment on the components of such a program, if any, and whether such a program would create business incentives for providers of communications services to sustain a high level of cyber security culture and practice. The Commission's goals in this proceeding are to: (1) Increase the security of the nation's broadband infrastructure; (2) promote a culture of more vigilant cyber security among participants in the market for communications services; and (3) offer end users more complete information about their communication service providers' cyber security practices. The Commission seeks comment on whether the program described herein would meet these goals. The Commission also seeks comment on other actions it should take, if any, to improve cyber security and to improve education on cyber security issues.

In today's interconnected world, an increasingly greater amount of the nation's daily business depends on our rapidly growing broadband communications infrastructure. Banking, investment and commercial interests routinely rely on the durability and security of IP-based networks to move capital and to track goods and services around the globe. To put this development in perspective, while our nation's total GDP was just over $14T last year, two banks in New York move over $7T per day in transactions. Moreover, our medical and educational establishments increasingly rely on robust broadband communications networks to reach distant patients and students in real time. Further, all levels of government, from the national to the local level, similarly depend on our communications networks to provide services, serve the public, collect information and maintain security. Such services require the instantaneous, secure movement of vast amounts of data.

The security of the core communications infrastructure—the plumbing of cyberspace—is believed to be robust. Yet recent trends suggest that the networks and the platforms on which Internet users rely are becoming increasingly susceptible to operator error and malicious cyber attack. For example, the Conficker botnet could be used to exploit vulnerabilities in underlying Internet routing technologies or other Internet mechanisms, thereby undermining the integrity of the Internet. There are also documented instances of distributed denial of service attacks on the Domain Name System infrastructure, a core Internet mechanism. Further, there recently has been an exponential growth in malware being reported. PandaLabs reports that in 2009 it detected more new malware than in any of the previous twenty years. It also reports that in 2009, the total number of individual malware samples in its database reached 40 million, and that it received 55,000 daily samples in its laboratory, with this figure rise in the most recent months. Unfortunately this growth also happens at a time when enterprises are spending less on security. Nearly half (47%) of all enterprises studied in the 2009 Global State of Information Security Study reported that they are actually reducing their budgets for information security initiatives. In addition, a 2008 Data Breach Investigation Report concluded that 87% of cyber breaches could have been avoided if reasonable security controls had been in place.

Given society's increasing dependence on broadband communications services and given trends suggesting our nation's increased susceptibility to operator error and malicious cyber attack, Federal entities, frequently in cooperation with the private sector, have been actively engaged in efforts to secure cyberspace. For example, the National Institute of Standards and Technology (NIST) has reached out to, and is using, private sector expertise to identify where barriers exist to information security standards development. The Federal Bureau of Investigation (FBI) has taken on a cyber mission that includes stopping those behind the most serious computer intrusions and the spread of malicious code, and the FBI together with Department of Justice lead the national effort to investigate and prosecute cybercrime. Moreover, the Department of Homeland Security's (DHS's) National Cyber Security Division has taken on the responsibility of seeking to protect the cyber security

of various critical sectors of the economy and government.

The Commission also has been part of Federal efforts to secure cyberspace, and already has taken a series of steps given its statutory duty to make available "a rapid, efficient, Nation-wide and world-wide wire and radio communication service with adequate facilities * * * for the purpose of the national defense [and] for the purpose of promoting safety of life and property through the use of wire and radio communication." 47 U.S.C. 151. First, the Commission was among the Federal agencies that contributed to the White House 60–Day Cyberspace Policy Review. This 60-day interagency document traced out a strategic framework to ensure that U.S. Government cyber security initiatives are appropriately integrated, resourced and coordinated with Congress and the private sector. Further, as his first act following confirmation, Chairman Julius Genachowski asked the Commission's Public Safety and Homeland Security Bureau (PSHSB or the Bureau) for an analysis and briefing within thirty days of his appointment on the FCC's preparedness for a major public emergency, including its preparation for, and response to, cyber emergencies.

In its report, PSHSB noted that while the Commission had taken some actions to address cyber security, it recommended that the Commission take steps to expand its role in this important area. The Bureau observed that one means by which the Commission has sought to motivate industry to adopt effective cyber security measures has been through the former Network Reliability and Interoperability Council (NRIC). In December 2004, NRIC began issuing an extensive set of best practices for securing computers and other software-controlled network equipment, which are referred to as cyber security best practices.

The Commission does not know whether there is wide-spread adherence to NRIC's cyber security best practices in the industry, or whether, if adopted, these best practices would be equally effective under all circumstances or for all broadband providers. The Commission believes that large organizations and commercial entities in particular are interested in the cyber security practices of their communications service providers, but notes that these customers of communications services have no effective way of knowing what the cyber security practices of competing providers may be. The lack of such information likely removes at least one significant incentive for providers fully to implement the NRIC best practices, in that they do not risk losing customers to networks with better security practices. The reduced incentive for heightened cyber security likely is compounded because a particular provider may not be motivated to exceed the security level of other interconnected network operators. Additionally, it appears that the sheer number of NRIC best practices may make it difficult for providers to prioritize them when determining how to invest their resources to improve network security. Moreover, the Commission's review of the best practices indicates that, in certain cases, they may provide too little specific guidance for network operators seeking to ensure that their operations meet objectively measurable cyber security criteria.

In its comprehensive *Broadband Notice of Inquiry* (NOI), 24 FCC Rcd 4342, the Commission posited a particular method of motivating broadband providers to adopt a cyber security culture. In the *Broadband NOI,* the Commission sought comment on the extent to which the Broadband Plan should address the cyber security issue, and if so, what steps the plan should take to secure the nation's most vulnerable broadband facilities and data transfers from cyber threats, such as espionage, disruption, and denial of service attacks. Specifically, the *Broadband NOI* asked whether the Commission should adopt a process whereby communications providers can certify their compliance with specific standards and best practices.

To ensure that end users are fully protected from attacks that affect or occur over communications infrastructure, the recently released *National Broadband Plan* (NBP) recommended that the Commission initiate a proceeding to establish a voluntary cyber security certification regime that creates market incentives for communications service providers to upgrade the cyber security measures they apply to their networks. In making this recommendation, the NBP stated that a voluntary cyber security certification program could promote a culture of more vigilant network security among market participants, increase the security of the nation's communications infrastructure and offer end users more complete information about their providers' cyber security practices. The NBP further recommended that the Commission examine additional voluntary incentives that could improve cyber security and improve education about cyber security issues, as well as inquire about the international aspects of a certification program. This NOI represents an initial and necessary step to implementing these recommendations and enhancing the cyber security of our Nation's communications systems.

Discussion

Legal Authority

The proposed certification program would further the Commission's core purposes as set forth in section 1 of the Communications Act: (1) The establishment of "a rapid, efficient, Nation-wide and world-wide wire and radio communication service with adequate facilities," (2) "the national defense," and (3) "promoting safety of life and property through the use of wire and radio communication." 47 U.S.C. 151. The Commission seeks comment on the strongest sources of authority to create the proposed certification program, if any, and asks commenters to address whether different sources of authority would be required with regard to program participation by different types of communications providers.

For example, the Commission seeks comment on whether the proposed certification program would fall within specific grants of authority in Title II and Title III. In addition, the Commission seeks comment on whether it could, if necessary, exercise ancillary authority to create a voluntary certification program. In particular, the Commission seeks comment on the scope of the Commission's ancillary authority, if any, to implement the proposed program in light of the recent decision of the United States Court of Appeals for the District of Columbia Circuit in *Comcast Corporation* v. *FCC.*

A Market-Based Incentives Program To Encourage Industry Cyber Security Practices

As noted above, the Commission seeks comment on whether the FCC should establish a voluntary incentives-based certification program in which participating communications service providers will receive network security assessments by approved, private-sector auditors who will examine those provider's adherence to stringent cyber security practices that have been developed, through consensus, by a broad-based public-private sector partnership. Those providers whose networks successfully complete the assessment may then market their networks as complying with stringent FCC network security requirements.

The Commission seeks comment on the benefits, advantages, disadvantages and costs of this program. For example, in proposing this program, the Commission hopes to create a

significant incentive for all providers to increase the security of their systems and improve their cyber security practices. Would the program envisioned meet this goal? Would such a program create an economic incentive that will lead service providers to implement best practices? Would it create incentives for small communications service providers? Would it create disadvantages for smaller communications service providers or present barriers to new entrants? If it does create such disadvantages and/or barriers, what can be done to mitigate such effects, if anything? What about those serving rural areas and/or tribal lands? The Commission also seeks comment on whether the public awareness of cyber security practices that could result from a cyber security certification program would contribute to broader implementation by industry.

Would an FCC cyber security certification be an important factor in service provider selection by major customers, including consumers, businesses and all levels of government? From an end user perspective, would the program the Commission envisions, with its focus on market-based incentives and consensus-based criteria, raise any concerns regarding the value of the program? If so, what actions could the Commission take, if any, to address those concerns, should it decide to move forward with establishing this program?

The Commission anticipates that a communications provider's participation in the certification program discussed herein would be voluntary, but that by agreeing to participate, such communications providers would be bound by the program's rules. The Commission seeks comment on this approach. Would the advantages of a voluntary cyber security certification program outweigh any disadvantages of a voluntary program, *i.e.,* that by its nature, it is not mandatory. Would a mandatory cyber security certification program better achieve the Commission's overall goals?

To offset the administrative costs associated with the voluntary certification program, should the Commission collect fees from those communications service providers that decide to participate? If so, how should such fees be determined and collected? Would the resultant costs outweigh the program's value to participants?

Scope of Participation

The Commission seeks comment on the scope of the certification program. Should the program, if implemented, be open to all communications service providers or should it be limited to certain types of providers? If the latter, which ones? Should it be focused on Internet Service Providers? The Commission observes that a program open to a more diverse set of entities may require the use of certification criteria that are so broad as to reduce the value of the certification program in the eyes of end-users and communications providers alike. Is there merit to this observation? Why or why not? Would restricting the applicants to Internet Service Providers permit a more focused, meaningful set of certification criteria? Should the Commission develop multiple sets of sector-specific certification criteria? The Commission anticipates that participation in this program, if established, would be limited to entities providing communications services within the United States and/or companies that own or operate communications assets in the United States, including non-U.S. entities that are authorized to do so. The Commission seeks comment on this approach.

General Network Cyber Security Objectives

Under the program envisioned, the Commission would establish general cyber security objectives that would serve as the starting point for the program. These objectives would serve as the overarching policy goals that would then form the basis for the criteria on which participating communications service providers would be assessed. The Commission seeks comment on whether general security objectives could serve as a sufficient basis for the cyber security certification program on which it seeks comment today. Can a set of general security objectives, by highlighting significant cyber security threat areas, serve as a guide by which communications providers can develop and implement specific, assessable cyber security policies and practices? The Commission seeks comment on the following four possible security objectives that it proposes as the starting point of the security regime: (1) Secure equipment management; (2) updating software; (3) intrusion prevention and detection; and (4) intrusion analysis and response. Are these sufficient as the initial set? Should there be more? Fewer? Commenters are encouraged to be specific on this issue.

Secure equipment management. The Commission recognizes that communications networks often rely on the ability to manage network equipment remotely and automatically; these capabilities can provide significant operational benefits. However, this remote management capability can also expose networks to significant risks of unauthorized access and systemic destruction. The Commission believes that good security practice directs network operators to install and maintain security management practices that cover all remotely managed equipment and to ensure, as fully as possible given current technologies, against damage or unauthorized access to network equipment.

Updating software. Keeping system software up to date is essential to continued security of the network, as new vulnerabilities regularly come to light after network operators have placed software in operation in their networks. Accordingly, proper network-security practices require comprehensive version management and the prompt installation of software updates that effectively address level and severity of the threat that a particular vulnerability poses.

Intrusion prevention and detection. Despite the best equipment management and patching practices, communications networks, by their very nature, will remain susceptible to intrusion and/or attack. Therefore, a necessary component of any security regime will be procedures to ensure timely and appropriate intrusion prevention, detection, and response. The Commission expects that these procedures will be calibrated to most quickly detect and respond to those network intrusions that, by virtue of their location, pose the greatest threat to the continued reliable and secure operation of the affected network.

Intrusion analysis and response. Physical damage or disruption of network components, whether the product is of natural or man-made events, poses another significant threat to our communications networks. Accordingly, proper network-security practices dictate that network operators be prepared to quickly recognize and respond in the event that network components sustain physical damage or experience degraded operating efficiency. This would include having appropriate redundancies built into the network and having adequate repair and replacement plans, as well as spare equipment and software, for network components likely to sustain physical damage.

Role for the Private Sector

Additionally, the Commission seeks comment on the role for the private sector that the Commission envisions in

this network-security regime. Should the private-sector bodies involved in this certification program have extensive responsibilities in this program, or should the Commission retain primary responsibility for the maintenance and administration of the proposed program? Given that the vast majority of U.S. communications infrastructure is privately controlled, once general cyber security objectives have been established could a certification authority—a private-sector body composed of major industry stake holders—responsibly take over the task of developing and maintaining the applicable security criteria? In particular, the Commission seeks comment on whether various private-sector entities (or the Commission) should: (1) Be responsible for developing, maintaining and improving the list of network cyber security criteria; (2) have responsibility for accrediting the auditors who will conduct security assessments of communications service providers; (3) establish the assessment procedures and practices to guide those assessments; and (4) maintain a database of the communications services providers that have passed the assessments and are therefore entitled to market their services as meeting the FCC's cyber security certification requirements. Which entity should actually grant certifications for the cyber security program? Should it be the Commission, and if not, what should be the characteristics of the entity that would best perform this function? Additionally, the Commission seeks comment on whether the auditors should also be private-sector entities. If so, in order to prevent conflicts of interest, should the Commission prohibit the program's auditors from being affiliated, or having other relationships, with any of the entities with responsibility for the various other aspects of the certification program or entities that are participating in the program?

The Commission seeks comment on whether significant private-sector involvement of this sort would serve the security goals of this program and thereby serve the public interest. While the Commission suggests that it may have the responsibility to establish or review the general security objectives and to serve as a final route of appeal when necessary, the Commission does not believe that it has the substantial resources needed to participate in the daily operation of the proposed cyber security certification program. On the other hand, the Commission believes that the private sector does have the resources necessary to keep such a program functioning quickly and efficiently. The Commission seeks comment on this issue. Furthermore, the Commission believes that manufacturers, users and communications providers have the most current knowledge of virtually every aspect of network technology. Accordingly, the Commission seeks comment on whether such private sector representatives would be able to contribute their up-to-date knowledge to the program in a way that would allow the program to be most effective in keeping pace with technological developments and in responding effectively to developing threats to the communications infrastructure. Would industry participants be concerned about their ability to share proprietary information in this way? How could the Commission alleviate these concerns, if at all, including through any structural safeguards? The Commission believes that this approach builds on its traditional approach to network reliability and security: the Commission has recognized industry's operational experience and personnel resources, and has applied them through mechanisms like the NRIC, MSRC, and most recently CSRIC. The Commission notes that it has previously charged the private sector with similar broad authority in the Part 68 mandatory certification regime governing the attachment of network terminal equipment. The Commission seeks comment on the feasibility and benefits of, and other relevant issues arising from, having the cyber security regime rely in this manner on the private sector, rather than primarily on Commission resources. The Commission also seeks comment on whether there exist any private entities that could perform the functions enumerated above. If so, who are they? If not, how could the Commission facilitate creation of such bodies, if at all?

A certification program along the lines contemplated could very well require a significant level of administrative activity. Keeping this in mind, should the Commission establish a certification administrative entity? If so, should the entity acting as the "administrator" be required, as part of its role, to establish and maintain a database of certificated networks/providers? More generally, what are the types of activities that should be performed by the program administrator?

Although the Commission anticipates that the certification regime it envisions would be primarily administered by the private sector, the Commission seeks comment on whether it should retain the ability to guide the development of the program through its continued review of the general security objectives. Additionally, the Commission seeks comment on whether as part of its oversight authority, it should be available as a final avenue of appeal for certain decisions by the certification authority, the auditors and the other entities involved in the program. Does the public interest require that the Commission maintain a greater level of scrutiny or control with respect to the activities of particular entities? If so, the Commission seeks comment on what particular scrutiny or control, if any, would best protect the public interest. For example, would it unnecessarily delay the functioning of the certification authority—and its ability to respond to new network security threats—for the Commission to formally seek public comment on certification criteria that the authority may develop in the future? Alternatively, would the Commission's ability to set the general network security objectives and adjudicate appeals from action of the certification authority, if such ability exists, permit the Commission adequately to protect the public interest by influencing the operation and direction of the cyber security regime?

Finally, it is possible that similar certification-related programs have already been implemented in the private sector. Are there existing industry-sponsored initiatives which seek to improve security and reliability of networks by certification, applying industry-established standards? If so, please comment on each initiative's scope, organization and participation. Comments are also requested on whether it would be beneficial and appropriate to utilize any relevant standards established by such groups in the Commission's cyber security certification program. Should the efforts of the Commission in the area of cyber security, if any, to establish a certification process for services providers be aligned with existing cyber security efforts either commercial or government, domestic or international? If so, which organizations should be considered and which specific points of alignment are relevant?

Security Criteria

As noted above, the Commission envisions that participating communications service providers would be assessed based on a stringent set of criteria. The Commission seeks comment on the overall framework for the certification criteria. What role, if

any, should a standards development body play in establishing the criteria to determine if an applicant to the certification program is "certification worthy," and if such a role is appropriate, which entity should be responsible for such development? Is it possible to assess different management and operational models with a single set of generic criteria that measure an organization's commitment to providing cyber security? Why or why not? Alternatively, should the set of criteria vary based on the specific nature of the applicant's business? The Commission observes that this latter method might better measure the extent to which relevant cyber security measures are applied at a particular entity, how could assessments based on different sets of criteria be compared?

The Commission seeks comment on possible criteria by which participating network operators would be assessed. The Commission believes that the assessment of any level of security must be based on objectively verifiable criteria. This assumes some kind of objectively accepted method of observing the network, for example, through direct examination by the Commission, reports by network providers and/or examination of the network by third parties. The Commission seeks comment on this view.

The Commission also seeks comment on how to ensure that any criteria adopted keeps up with not only current but also evolving threats and technology. To obtain certification, should the Commission require a showing that certain defense-in-depth steps or measures have been taken, ones that are reasonably available and can deter/prevent certain types of hacking and other security breaches of broadband Internet services? For example, one existing cyber threat, "MAC spoofing," is a technique whereby cyber hackers can remotely change an assigned Media Access Control address of a network device to a different one, allowing the cyber intruder to bypass access control lists on servers or routers, either "hiding" a computer on a network or allowing it to impersonate another computer. This technique can be not only harmful to the end user, but it can threaten the ability of the service provider's network to function as designed and to be available when required. Before a service provider applicant is granted a certificate, should the applicant be required to demonstrate particular best practices or other steps that have been taken to avert MAC spoofing, enhance detection of it, and take effective corrective action once detected?

As Americans increasingly rely on broadband technology and IP-enabled services in their everyday lives, they will want greater transparency from service providers. More specifically, consumers will want to be able to compare and judge the quality and robustness not only of the IP-enabled services provided by various providers, but also of the providers' cyber security programs, and related data (*e.g.* number of outages, number of security breaches, *etc.*) that may affect them. If greater transparency is expected from service providers, the providers would have incentive to improve their performance, and consumers would have access to important information unrelated to price, which to date has been difficult for them to obtain. Comments are requested on how the criteria could be structured to reward greater transparency among service providers so that consumers are able to obtain important types of data needed to guide their decisions on provider selection and on the extent to which they can reasonably rely on the security of their IP-enabled services.

Alternatively, would a program based on the sorts of general cyber security objectives described above be effective? Could these general cyber security objectives serve as the basis of a case by case inquiry to measure the specific cyber security practices of individual communications providers? Assuming that it would be possible to arrive at cyber security criteria based on a mutually agreed upon set of general objectives, the Commission seeks comment on whether such security objectives could serve as the basis for a set of specific network cyber security criteria against which it would be possible to objectively measure the network-security practices of communications service providers. If so, could NRIC or CSRIC best practices serve as the criteria for a cyber security certification program? If not could the Commission establish a set of cyber security criteria?

The Commission seeks comment on the procedure for updating the certification criteria or objectives. Should a single certification authority have ongoing responsibility for keeping the certification criteria in step with new developments in technology? Could it constantly apply the industry's evolving knowledge of how best to combat the most recent security threats? Whether such authority resides in an independent entity or the Commission, it will therefore be necessary to update the certification criteria on a regular basis. The Commission seeks comment on how this should occur.

Structure of Security Regime

Membership. Given the central importance of the criteria to the continuing success of a cyber security certification program, it is important for the entity developing them to have access to as broad of a range of knowledge and experience in the relevant fields as possible. If a certification authority is established, the Commission believes that it should be fairly balanced in terms of the points of view and industry segments that sit on it. Accordingly, the Commission seeks comment on whether a certification authority should be open to all segments of the potentially affected industries, including incumbent and competitive wireline carriers; wireless and satellite providers; cable service providers; undersea cable operators, internet service providers (both facility and non-facility based); and providers of VOIP services. The Commission seeks comment on whether any other potentially interested groups or entities should also be involved.

The Commission recognizes that a body representing so many diverse interests runs the risk of growing too large to be able to function effectively. Accordingly, the Commission seeks comment on how to ensure that a certification authority can be limited to a workable size without having the unintended result of arbitrarily restricting the participation of interests that should be involved in the authority's activities. The Commission also seeks comment on the applicability to the certification authority of the membership criteria set out in International Standard ISO/IEC 17011(E), particularly sections 4.2 (Structure) and 4.3 (Impartiality).

Assuming a certification authority possessed the significant degree of autonomy on which the Commission seeks comment, would it be necessary for the Commission to prescribe other rules regarding membership, such as procedures for admitting new members or time limits on the service of particular entities and individuals?

Operating Procedures. Having charge, as it would, of the centerpiece of the cyber security regime, a certification authority would have the potential for significant impact—both positive and negative—on numerous entities in the communications industry. Accordingly, the Commission seeks comment on whether it would be necessary for the authority to reach its decisions through a process that appropriately preserves the rights of all affected parties. For

example, the American National Standards Institute (ANSI) has developed procedures to assist decision-making by consensus. In particular in the *Part 68 Order,* the Commission discussed the benefits of the Organization Method and the Standards Committee Method, both of which provide procedures to help ensure equal participation by entities participating in decision-making in large, diverse bodies. These ANSI procedures offer an array of due process protections. The Commission seeks comment on whether these decision-making requirements and/or any others should apply to the operations of the certification authority:

a. The right of any person (organization, company, government agency, individual, *etc.*) with a direct and material interest to participate by expressing an opinion and its basis, having that position considered, and appealing if adversely affected.

b. No undue financial barriers to participation, no conditions upon participation based on organization membership, and no unreasonable requirements for technical qualifications, *etc.*

c. A requirement that the standards development process include a balance of interests and that it not be dominated by any single interest category.

d. A requirement to actively seek and fully consider relevant, representative user views including individuals and organizations.

e. A requirement that written procedures govern the methods used for standards development and will be available to any interested person.

f. A requirement that the written procedures contain an identifiable, realistic, and readily available appeals mechanism for the impartial adjudication of substantive and procedural complaints regarding any action or inaction.

g. Notification of standards activity shall be announced in suitable media; comment periods are specified.

h. A requirement that prompt consideration be given to the written views and objections of all participants; a prompt effort shall be made to resolve all objections; each objector shall be informed in detail of the appeals process and how to proceed if the objector so desires.

i. International standards shall be taken into consideration.

j. The principle that it is generally not acceptable to include proper names or trademarks of specific companies in a standard, but a patented item may be used in a term if technical reasons justify this approach.

The Commission also seeks comment on whether ANSI accreditation procedures should formally apply to the certification authority. If so, should it be the Organization Method or the Standards Committee Method that applies?

As noted above, the Commission seeks comment on whether a cyber security certification authority and the entities serving on it be prohibited from serving as auditors under the program. Would such a restriction help reduce the potential for conflicts of interest or claims of undue influence in the process? The Commission seeks comment on this aspect of the proposal.

Auditor Accreditation. As set out above, stringent, objective assessments of individual providers would compose an important part of the cyber security certification program on which the Commission seeks comment herein. Accordingly, should an independent auditor accreditation body, composed of private-sector entities with relevant expertise, be responsible for establishing the requirements that auditors must meet to be accredited to conduct cyber security assessments under the regime proposed today? Should the Commission delegate the precise details about the structure of the accreditation process to an accreditation body? The Commission anticipates, however, that the accreditation process will involve the advance publication of specific standards for the auditors involved in the program and an application and approval process through which auditors may seek inclusion on the list of those entities that have received official approval to conduct network security assessments. The Commission seeks comment on the foregoing aspects of the program. Should the Commission impose requirements on the auditor accreditation process to ensure competence, integrity and objectivity in the accreditation of auditors? If not, why should the Commission choose not to impose such requirements? In addition, should the Commission impose these requirements for auditor qualification in the application or approval process? Should it require that a certain number of auditors be accredited before the assessment or accreditation process may begin? Additionally, the Commission seeks comment on whether the auditor accreditation body should be required to meet the requirements and conditions of International Standard ISO/IEC 17011:2004(E) to the extent that it serves as an accreditation body for compliance auditors in this program.

Given the narrow, specialized focus of the auditor accreditation body, the Commission expects that it will be appropriate for membership to differ substantially from that of the certification authority discussed above (both in the entities that are represented in each, as well as the individuals who would be involved in each activity). More generally, the Commission seeks comment on the appropriate composition of this body. What entities or industry segments should be represented on it? Should the Commission limit the body's size, given the relatively narrow focus of its work? As with the certification authority, the Commission proposes that members of the accreditation body and their affiliates be prohibited from serving as auditors in the cyber security program. Should the Commission place any other limitations on the membership of the accreditation body?

The Commission seeks comment on whether the accreditation body should follow the consensus decision-making model discussed above in connection with the certification authority. The Commission seeks comment on whether it is necessary for it to provide any additional guidance on the operating procedures for the auditor accreditation body.

Development of Assessment Standards. It would, of course, be necessary to develop assessment standards to guide the auditors' review of the cyber security measures of participating providers. As indicated above, the Commission seeks comment about whether the network-security criteria will be definitive and objectively measurable. The Commission has sought comment on whether it is feasible to establish such criteria, either on an objective, generally applicable basis, or on a case by case basis by using general cyber security objectives. Either way, the auditors likely will need additional guidance about how to apply the security criteria to particular providers. What role, if any, should a standards body play in this process? Should certain criteria only be applicable to specific types of providers? Should assessment standards set out which criteria apply to which types of providers? Additionally, the Commission seeks comment on whether it would be necessary to establish: (1) What portion of the applicable assessment criteria a provider must pass in order to successfully complete the assessment; (2) what percentage of a provider's operations the auditors must examine for compliance with applicable security criteria; (3) whether any level of self-certification by providers will be permitted on any of the assessment criteria; and (4) whether a particular assessment will be an "examination

engagement" or an "agreed upon procedures audit."

If the certification program specifies only general security criteria, it may be necessary for the applicant to define in greater detail the specific security measures that would satisfy those general criteria. In such circumstances, a two-step process may be necessary: First, the certification authority would review and approve the applicant's proposed specific criteria, to ensure that they truly satisfy the general security criteria; and second, it would review and approve the applicant's satisfaction of those criteria. The Commission seeks comment on such an approach. Are there ways to minimize the need for applicants to self-define specific security criteria? Could the examination function of the certification entity consist mainly of approving the applicant's internal audit? Would this be a more efficient, less burdensome approach? The Commission believes that an objectives-based certification would give the certifying entity significant discretion to determine whether an applicant had satisfied a particular objective. Should there be some level of oversight to this discretion, either by an applicant appeal or by Commission review? The Commission seeks comment on these questions.

Should the auditor accreditation body also develop these assessment standards, or should they be developed by a separate entity? If it is appropriate to constitute a separate entity for this task, the Commission seeks comment on the appropriate composition of such a body. Again, in light of the narrow focus of such a body, the Commission expects that this body likely would have a more limited membership than the proposed certification authority. Should the group developing assessment standards be required to involve members of the professional auditing community in some of these decisions, and, if so, how?

Should the Commission prohibit the members of the assessment standards body and their affiliates from serving as auditors in the network security program? Should the Commission set additional limitations on the membership or operations of such a group? Should it direct the group to operate according to the consensus model discussed above in connection with the certification authority?

Should the Commission seek public comment on proposed assessment criteria before they go into effect? Should the Commission exercise some other form of control or guidance over the development of the assessment criteria? As with the security criteria, the Commission also seeks comment on how frequently and through what mechanism the assessment procedures should be updated.

Maintaining Assessment Results; Conferring Security Certificate. The final aspect of the network security program that the Commission proposes involves keeping records of successful assessment results. It appears that a database administrative entity may not need to possess the detailed results of the security assessment in order to perform its job of maintaining a publicly available database, but it also appears that both the audit plan for a particular communications service provider and the detailed results of an audit might well need to be preserved and made available to the Commission upon request. To that end, who should be responsible for keeping the detailed records? Who besides the Commission should be allowed access to such records? Upon the successful completion of a security assessment, should the auditor and the network operator jointly communicate the assessment results to an appropriate entity? Would the appropriate authority's receipt of this NOI be the event that entitled the communications service provider to begin marketing its services as having received the FCC's network-security certification? Under this approach, would it be necessary for the Commission to receive notification of, or to confirm, the assessment results? Rather, should some private entity be responsible for creating and maintaining a publicly available database of the communications service providers that have met the applicable network security criteria by virtue of a successful assessment? The Commission seeks comment on this structure of the network security program, the retention of assessment results, the frequency with which entities must be recertified that have successfully completed the assessment certification process, and any requirements for upgrading security. For example, should recertification require upgrading of security based on products that are used in the market place? Should the certification process require that updates be applied before the onset of the next certification cycle? The Commission seeks comment on whether it should designate some entity, such as a standards development body, to perform this function or whether it should be done by the certification authority or some member thereof, if anything.

Should the Commission seek to develop a process to track the effectiveness of the certification process with regard to improvements in cyber security realized, the cost to implement, and other factors that would seek to quantify the overall effectiveness of the program? If so, what factors should be considered, if any?

Appeals to the Commission

Although the Commission has sought comment on a cyber security certification program as being largely a private sector process, it also seeks comment on whether public interest considerations would support giving participating parties the right to appeal adverse decisions to the Commission. For example, should parties be able to bring to the attention of the Commission instances in which they feel the certification authority has been either too strict or too lax in defining the security criteria? Should they be permitted to challenge assessment procedures; the accreditation of auditors; and the final result of an assessment? Should an aggrieved party be required initially to present its appeal to, and obtain a decision from, the certification authority, or other relevant program entity, before applying to the Commission for review? Should appeals to program authorities be subject to some relatively short deadline? Similarly, should appeals to the Commission be permitted only if filed within a limited period of time after the appeal decision of the relevant security program authority? The Commission seeks comment on this aspect of the proposed program and the time periods that would be appropriate.

Security Certificate

Several additional questions arise in connection with the security certificate that would be conferred on providers that have successfully completed an assessment under the cyber security certification program. First, what should be the duration of the certificate? The Commission recognizes that communications technology and threats to cyber security are constantly evolving. Accordingly, it is reluctant to adopt a regime in which the certificate lasts for too long. Such an arrangement might reduce a provider's incentive to stay abreast of the latest industry developments. On the other hand, the Commission acknowledges that too short of a certification period (and the attendant repeat assessment obligation) might depress participation in this voluntary program. In attempting to balance these competing considerations, how long should the security certification last, after which a communications service provider would be required to pass another assessment?

The Commission seeks comment on this issue.

A related issue on which the Commission seeks comment is the appropriate renewal process for the security certification. The Commission seeks comment on whether the initial assessment of a provider's network security practices will be relatively extensive. The Commission seeks further comment on whether the assessment preceding renewal of a security certification should be more truncated. Alternatively, should a provider be permitted a greater level of self-certification in connection with a certificate renewal? Is the question of certificate renewal procedures one that the Commission should leave to the certification authority or the assessment standards body, or should the Commission, if anything, set certain threshold requirements on which the appropriate program authority can build later?

The Commission also seeks comment on the permissible uses by providers of the security certification. As discussed above, the Commission envisions that the program, if implemented, would permit communications service providers to distinguish their services in the marketplace by advertising them as compliant with FCC-sanctioned security requirements. Is it necessary or appropriate to place limits on the manner in which providers that have received a certificate may use it? Is doing so consistent with applicable legal, including Constitutional, constraints on the Commission's action?

The Commission seeks comment on what form the evidence of the security certificate should take. The Commission presently expects that it will develop an appropriate logo or emblem, analogous to that used for Part 15 devices, which a provider would display to indicate that it had received the security certification. Should an emblem of this sort be accompanied by short, stock text describing the security certification? If so, the Commission seeks comment on the appropriate phrasing.

Enforcement Matters

The Commission seeks comment on whether any Commission enforcement process should accompany the cyber security certification process. For example, would it be necessary for the Commission, if anything, to have in place special procedures to address the situation if a provider incorrectly claims to have received the security certificate? Or, would it be sufficient for the certification authority and/or the Commission, if anything, to publish a statement correcting the provider's incorrect statement? In addition, the Commission seeks comment as to what enforcement process should be followed, if any, and what action, if any, should be taken for attempted misuse or actual misuse of the security certification or seal. How should applicants be treated who apply for certifications under false pretenses? What action, if any, should be taken if a communications service provider were to hold itself out to the public as having such a certification without being properly certified?

The Commission expects that it would be unnecessary for it to have a separate enforcement process for the auditors in a cyber security certification program. Rather, the Commission expects that an auditor dissatisfied with a decision of the certification authority—presumably a decision to exclude the auditor from participation in the security certification program—would simply petition the Commission like any other dissatisfied party. The Commission seeks comment on this question. Is it necessary for the Commission to create any other mechanisms relating to dispute resolution specific to this program?

Should the Commission, or a private sector entity, be responsible for deciding to revoke, suspend, or reinstate a revoked security certificate? If a certificate is suspended, how long should suspension last? If a certificate is revoked, how long should the service provider be required to wait before the Commission allows that provider to re-apply for certification? Given that certifications may last for a particular duration and may possibly be renewed, several questions arise. Should a procedure be established to revoke or suspend a security certificate before its expiration date and, if so, what should the process entail? Should the Commission consider, if anything, revoking or suspending a security certificate for repeated network outages for violation(s) of the program's best practices/standards? What kinds of record-keeping or other requirements, if any, should be imposed on certificate holders in order to make the determination that a certificate should be revoked or suspended? The Commission seeks comment on these questions and on other actions it can take in this area.

Domestic and International Coordination

The Commission recognizes that increasingly, broadband networks used by U.S. ISPs are connected to many other networks, including the electric grid and the financial sector. These connections exist within the United States as well as between the United States and other countries. The Commission seeks comment on cyber security efforts underway for these interconnected networks that could inform the certification program, as well as ways the Commission might wish to coordinate, if at all, the development of its certification program, if any, with firms and agencies related to these networks. The Commission also recognizes that work on the subject of cyber security is currently underway in various countries and in international organizations such as the International Telecommunications Union (ITU) and Organisation of Economic Cooperation and Development (OECD). The Commission invites comment on how those work efforts could inform the FCC's certification program, if at all, and how the Commission could share the expertise gained from this program with other countries and international organizations, if at all.

Other Cyber Security Incentives

Apart from the issue of a certification program, the Commission seeks comment on other actions, including voluntary incentives the Commission can take to improve cyber security, if any. Are there effective and efficient methods that the Commission should consider, if any, that could ensure the cyber security of commercial broadband networks as they relate to national purposes such as public safety, consumers, healthcare, education, energy, government and security? Commenters suggesting ideas should provide details of their suggestions, including the benefits, advantages, disadvantages and costs. The Commission is interested not only in actions it can take on its own, but also ideas that the Commission might recommend to its Federal partners or to Congress, if any. The Commission also seeks comment on how to improve education on cyber security issues. What actions, if any, can the Commission take to better educate end users, including consumers, businesses and government agencies about cyber security? Are there, for example, educational and/or outreach activities in which the Commission, either alone or with other stakeholders (*e.g.,* Federal agencies, state and local governments, private industry) should engage to assist individuals in protecting their personal computers and other devices? How can the Commission better educate the industry about best practices and other methods to enhance cyber security in their communications networks and systems, if at all?

The Commission further notes that cyber threats to network end users also threaten the abilities of the service provider's network to function as designed and to be available when required. Such threats include, for example, the proliferation of botnets and from "MAC spoofing," a technique whereby cyber hackers remotely change an assigned Media Access Control address of a network device to a different one, allowing the bypassing of access control lists on servers or routers, either "hiding" a computer on a network or allowing it to impersonate another computer. Therefore, the Commission seeks comment on steps that service providers should take, if any, to help detect and respond to threats to end users that take place *on or through* the service provider's network, and the extent to which best practices in this area would enhance detection and maximize effectiveness of response.

Procedural Matters

Ex Parte Presentations. This matter will be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules. *See* 47 CFR 1.1200 & 1.1206. Although a Notice of Inquiry proceeding is generally exempt from the *ex parte* rules, the Commission finds that the public interest is best served by treating this critical cyber security matter as a "permit-but-disclose" proceeding. *See* 47 CFR 1.1200(a), 1.1204(b)(1). Persons making oral *ex parte* presentations are reminded that memoranda summarizing the presentations must contain summaries of the substance of the presentations and not merely a listing of the subjects discussed. More than a one- or two-sentence description of the views and arguments presented is generally required. Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in § 1.1206(b) of the Commission's rules, 47 CFR 1.1206(b).

Comment Filing Procedures. Comments may be filed using: (1) The Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies. *See Electronic Filing of Documents in Rulemaking Proceedings,* 63 FR 24121 (1998). Comments may be filed electronically using the Internet by accessing the ECFS: *http://fjallfoss.fcc.gov/ecfs2/* or the Federal eRulemaking Portal: *http://www.regulations.gov.* Parties who choose to file by paper must file an original and four copies of each filing.

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. Effective December 28, 2009, 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. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes 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.

Ordering Clause

Accordingly, it is ordered that, pursuant to sections 1, 4(i), 4(j), 4(o) and 7(b), 403 of the Communications Act of 1934, as amended, 47 U.S.C. 151, 154(i)–(j) & (o), 157(b) and 403, this Notice of Inquiry is adopted.

Federal Communications Commission.

Marlene H. Dortch,

Secretary.

[FR Doc. 2010–11162 Filed 5–10–10; 8:45 am]

BILLING CODE 6712–01–P

FEDERAL COMMUNICATIONS COMMISSION

47 CFR Chapter I

[PS Docket No. 10–92; FCC 10–62]

Effects on Broadband Communications Networks of Damage To or Failure of Network Equipment or Severe Overload

AGENCY: Federal Communications Commission.

ACTION: Proposed rule.

SUMMARY: Consistent with the recommendations of the National Broadband Plan, the Federal Communications Commission (Commission or FCC) adopted this Notice of Inquiry to seek comment on the present state of survivability in broadband communications networks and to explore potential measures to reduce network vulnerability to failures in network equipment or severe overload conditions, such as would occur in natural disasters, pandemics, and other disasters or events that would restrain our ability to communicate. The Commission seeks comment broadly on the ability of existing networks to withstand localized or distributed physical damage, including whether there is adequate network redundancy and the extent of survivability of physical enclosures in which network elements are located, and severe overloads.

DATES: Comments are due on or before June 25, 2010 and reply comments are due on or before July 26, 2010.

ADDRESSES: Comments and reply comments may be filed using: (1) The Commission's Electronic Comment Filing System (ECFS), (2) the Federal Government's eRulemaking Portal, or (3) by filing paper copies.

Comments and reply comments may be filed electronically using the Internet by accessing the ECFS: *http://fjallfoss.fcc.gov/ecfs2/* or the Federal eRulemaking Portal: *http://www.regulations.gov.*

Parties who choose to file by paper can submit filings 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. All hand deliveries must be held together with rubber bands or fasteners. Any envelopes 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. Parties who choose to file by paper must file an original and four copies of each filing.

Parties wishing to file materials with a claim of confidentiality should follow the procedures set forth in § 0.459 of the Commission's rules. Confidential submissions may not be filed via ECFS but rather should be filed with the Secretary's Office following the procedures set forth in 47 CFR 0.459. Redacted versions of confidential submissions may be filed via ECFS.

FOR FURTHER INFORMATION CONTACT: John Healy, Communications Systems Analysis Division, Public Safety and Homeland Security Bureau at 202–418–2448 or Jeffery Goldthorp, Chief, Communications Systems Analysis