DOCKET FILE COPY ORIGINAL

Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
	)	PS Docket No. 10-93
Cyber Security Certification Program	)	
	)	

MAILED
APR 26 2010
FCC Mail Room

NOTICE OF INQUIRY

Adopted: April 21, 2010 **Released: April 21, 2010**

Comment Date: [60 days from date of publication in the Federal Register]
Reply Comment Date: [120 days from date of publication in the Federal Register]

By the Commission: Chairman Genachowski and Commissioners Copps, McDowell, Clyburn, and Baker issuing separate statements.

TABLE OF CONTENTS

Heading Paragraph #

I. INTRODUCTION 1
II. BACKGROUND 2
III. DISCUSSION 10
A. Legal Authority 10
B Market-Based Incentives Program to Encourage Industry Cyber Security Practices 12
C. Scope of Participation 17
D. General Network Cyber Security Objectives 18
E. Role for the Private Sector 23
F. Security Criteria 28
G. Structure of Security Regime 34
1. Auditor Accreditation 38
2. Development of Assessment Standards 41
3. Maintaining Assessment Results; Conferring Security Certificate 46
H. Appeals to the Commission 50
I. Security Certificate 51
J. Enforcement Matters 55
K. Domestic and International Coordination 58
L. Other Cyber Security Incentives 59
IV. PROCEDURAL MATTERS 61
A. Ex Parte Presentations 61
B. Comment Filing Procedures 62
C. Accessible Formats 63
V. ORDERING CLAUSE 64

I. INTRODUCTION

1. This notice of inquiry seeks comment on whether the Commission should establish a voluntary program under which participating communications service providers[1] 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. We seek 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.[2] Our goals in this proceeding are: (1) to increase the security of the nation's broadband infrastructure; (2) to promote a culture of more vigilant cyber security among participants in the market for communications services; and (3) to offer end users more complete information about their communication service providers' cyber security practices. We seek comment on whether the program described herein would meet these goals. We also seek comment on other actions the Commission should take, if any, to improve cyber security and to improve education on cyber security issues.

II. BACKGROUND

2. 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.[3] 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.

3. 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[4] reports that in 2009 it detected more new malware than in any of the previous twenty years.[5] It also reports that in 2009, the total number of individual malware samples in

[1] By the term "communications service provider" we mean an entity that provides communications service by radio, wire, cable, satellite, and/or lightguide for a fee to one or more unaffiliated entities.

[2] "The best way for government to motivate the specific cyber security behaviors it would like industry to adopt to meet the national... interests, is to engage industry at the business plan level and make it in the private corporation's best economic interests to enhance the infrastructure." *Implementing the Obama Cyber Security Strategy via the ISA Social Contract Model,* Internet Security Alliance, 2009, available at www.isalliance.org/images/stories/downloads_pdf/Implementing_the_Obama_Cyber_Security_Strategy.pdf (last viewed Mar. 5, 2010).

[3] Testimony of Michael McConnell, former Director of National Intelligence, before the U.S. Senate Committee on Commerce, Science & Transportation (Feb. 24, 2010).

[4] PandaLabs is the anti-malware laboratory of Panda Security, a computer security company.

[5] Annual Report, PandaLabs 3 (2009), available at www.pandasecurity.com/img/enc/Annual_Report_Pandalabs_2009.pdf.

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.[6] 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.[7] 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.[8]

4. 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)[9] has reached out to, and is using, private sector expertise to identify where barriers exist to information security standards development.[10] The Federal Bureau of Investigation (FBI) has taken on a cyber mission that includes "stop[ping] 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.[11] 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.[12]

5. 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."[13] First, the Commission was among the Federal agencies that contributed to the White House 60-Day Cyberspace Policy Review.[14] This 60-day interagency document traced out a strategic framework to ensure that U.S. Government cyber security initiatives are appropriately

---

[6] *Id.*

[7] Testimony of Larry Clinton, President and Chief Executive Officer of the Internet Security Alliance, before the U.S. Senate Judiciary Committee (Nov. 17, 2009).

[8] Verizon Business, 2008 Data Breach Investigations Report 2-3 (2008), *available at* http://www.verizonbusiness.com/resources/security/databreachreport.pdf.

[9] NIST has statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, P.L. 107-347. NIST is responsible for developing standards and guidelines for providing adequate information security for all agency operations and assets, but such standards and guidelines do not apply to national security systems. *See* Testimony of W. Wyatt Starnes, Founder, President and CEO of SignaCert, Inc., before the U.S. House of Representatives Subcommittee on Technology and Innovation, House Committee on Science and Technology (Oct. 22, 2009).

[10] Testimony of Cita M. Furlani, Director of Information Technology Laboratory, NIST, before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology (July 21, 2009). As of July 21, 2009, there were four standards activities ongoing. Although standards are being developed by different standards bodies, there is "significant interaction among the working groups." *Id.*

[11] FBI website, http://www.fbi.gov/cyberinvest/cyberhome.htm (last visited Mar. 9, 2010).

[12] *See* DHS website, http://www.dhs.gov/xabout/structure/editorial_0839.shtm (last visited Mar. 9, 2010).

[13] 47 U.S.C. §151.

[14] *See* Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (White House, 2009).

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 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.[15]

6. In its report, the Bureau 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.[16] 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).[17] 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.

7. We do 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. We believe that large organizations and commercial entities in particular are interested in the cyber security practices of their communications service providers, but note 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, our 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.

8. In its comprehensive *Broadband Notice of Inquiry* (NOI), 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.[18]

9. To ensure that end users are fully protected from attacks that affect or occur over communications infrastructure, the recently released *National Broadband Plan*[19] (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

[15] *See* FCC Preparedness for Major Public Emergencies (FCC, September 2009).

[16] *Id.*, at pages 26-27.

[17] NRIC Best Practices are available at https://www.fcc.gov/nors/outage/bestpractice/BestPractice.cfm .

[18] *See* A National Broadband Plan for Our Future, GN Docket No. 09-51, *Notice of Inquiry*, FCC 09-31, ¶ 73 (rel. April 8, 2009).

[19] Omnibus Broadband Initiative, Federal Communications Commission, Connecting America: The National Broadband Plan (2010) at § 16.7.

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.[20] The NBP further recommended that the Commission examine additional voluntary incentives that could improve cyber security and improve education about cybersecurity issues, as well as inquire about the international aspects of a certification program. This Notice of Inquiry (NOI) represents an initial and necessary step to implementing these recommendations and enhancing the cyber security of our Nation's communications systems.

III. DISCUSSION

A. Legal Authority

10. 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."[21] We seek comment on the strongest sources of authority to create the proposed certification program, if any, and we ask commenters to address whether different sources of authority would be required with regard to program participation by different types of communications providers.

11. For example, we seek comment on whether the proposed certification program would fall within specific grants of authority in Title II[22] and Title III.[23] In addition, we seek comment on whether

[20] *Id.*

[21] 47 U.S.C. § 151.

[22] For example, section 201(b) requires that all practices of common carriers in connection with interstate or foreign communication by wire or radio be "just and reasonable." 47 U.S.C. § 201(b). Section 214 authorizes the Commission to require a common carrier "to provide itself with adequate facilities for the expeditious and efficient performance of its service." *Id.* § 214(d). Section 215 charges the Commission to "examine into transactions entered into by any common carrier which relate to the furnishing of equipment, supplies [or] services" which may affect the carrier's services, *id.* § 215(a), and section 218 empowers the Commission to inquire "as to technical developments and improvements in wire and radio communications and radio transmission of energy to the end that the benefits of new inventions and developments may be made available to the people of the United States," *id.* § 218. We note that section 218 casts a relatively wide net, permitting the Commission to obtain such information from a broad range of entities affiliated with carriers subject to the Act.

[23] Under Title III, the Commission has the authority to establish operational obligations for licensees that further the goals and requirements of the Act if the obligations are in the public interest and do not contradict any basic parameters of the agency's authority. *See, e.g.*, 47 U.S.C. §§ 301 (granting the Commission authority over "radio communications" and "transmission of energy by radio"); 303(b) (authorizing the Commission, subject to what the "public interest, convenience, or necessity requires," to "[p]rescribe the nature of the service to be rendered by each class of licensed stations and each station within any class"); 303(r) (authorizing the Commission to "prescribe such restrictions and conditions, not inconsistent with law, as may be necessary to carry out the provisions of this Act"); 307(a) (authorizing the issuance of licenses "if public convenience, interest, or necessity will be served thereby"); 309(a) (authorizing the Commission to grant licenses when "the public interest, convenience, and necessity would be served"); 309(j)(3) (in specifying the characteristics of licenses, the Commission must "include safeguards to protect the public interest in the use of the spectrum and shall seek to promote the purposes specified in section 1 of this Act"); 316(a) (authorizing modifications of licenses if "in the judgment of the Commission such action will promote the public interest, convenience, and necessity"). *See also Schurz Communications, Inc. v. FCC*, 982 F.2d 1043, 1048 (7th Cir. 1992) (Communications Act invests Commission with "enormous discretion" in promulgating licensee obligations that the agency determines will serve the public interest). Title III of the Act also empowers the (continued....)

the Commission could, if necessary, exercise ancillary authority to create a voluntary certification program.[24] In particular, we seek 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*.[25]

B. A Market-Based Incentives Program to Encourage Industry Cyber Security Practices

12. As noted above, we seek comment on whether the Commission 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.

13. We seek comment on the benefits, advantages, disadvantages and costs of this program. For example, in proposing this program, we hope to create a significant incentive for all providers to increase the security of their systems and improve their cyber security practices. Would the program we envision 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? We also seek 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.

14. 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 we envision, 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?

15. We anticipate that a communications provider's participation in the certification program we discuss today would be voluntary, but that by agreeing to participate, such communications providers would be bound by the program's rules. We seek 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?

16. 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

(Continued from previous page)
Commission to regulate devices capable of causing "harmful interference to radio communications." 47 U.S.C. § 302(a).

[24] The Commission may exercise ancillary authority over a matter when it falls within the agency's general statutory grant of jurisdiction under Title I and the regulation is reasonably ancillary to the effective performance of the Commission's statutory responsibilities. *United States v. Southwestern Cable Co.*, 392 U.S. 157, 172–73 (1968); *accord United States v. Midwest Video Corp.*, 406 U.S. 649, 662 (1972). *See also American Library Ass'n. v. F.C.C.*, 406 F.3d 689, 691-92 (D.C. Cir. 2005).

[25] No. 08-1291, 2010 WL 1286658 (D.C. Cir. April 6, 2010).

so, how should such fees be determined and collected? Would the resultant costs outweigh the program's value to participants?

C. Scope of Participation

17. We seek comment on the scope of the certification program. Should the program, if implemented, be open to all communications service providers[26] or should it be limited to certain types of providers? If the latter, which ones? Should it be focused on Internet Service Providers? We observe 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 we develop multiple sets of sector-specific certification criteria? We anticipate 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. We seek comment on this approach.

D. General Network Cyber Security Objectives

18. Under the program we envision, 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. We seek comment on whether general security objectives could serve as a sufficient basis for the cyber security certification program on which we seek 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? We seek comment on the following four possible security objectives that we propose 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.

19. *Secure equipment management.* We recognize 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. We believe 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.

20. *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.

21. *Intrusion prevention and detection.* Despite the best equipment management and patching practices, communications networks, by their very nature, will remain susceptible to intrusion

[26] As noted in note 1, *infra*, the term "communications service provider" refers to an entity that provides communications service by radio, wire, cable, satellite, and/or lightguide for a fee to one or more unaffiliated entities.

and/or attack. Therefore, a necessary component of any security regime will be procedures to ensure timely and appropriate intrusion prevention, detection, and response. We expect 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.

22. *Intrusion analysis and response.* Physical damage or disruption of network components, whether the product 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.

E. Role for the Private Sector

23. Additionally, we seek comment on the role for the private seetor that we envision 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, we seek 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, we seek comment on whether the auditors should also be private-sector entities. If so, in order to prevent conflicts of interest, should we 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?

24. We seek 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 we suggest that the Commission may have the responsibility to establish or review the general security objectives and to serve as a final route of appeal when necessary, we do not believe that the Commission has the substantial resources needed to participate in the daily operation of the proposed cyber security certification program. On the other hand, we believe that the private sector does have the resources necessary to keep such a program functioning quickly and efficiently. We seek comment on this issue. Furthermore, we believe that manufacturers, users and communications providers have the most current knowledge of virtually every aspect of network technology. Accordingly, we seek 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? We believe that this approach builds on the Commission's 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. We note that the Commission has previously charged the private sector with similar broad authority in the Part 68 mandatory certification regime governing the attachment of network terminal equipment.[27] We seek 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. We also seek 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?

25. 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?

26. Although we anticipate that the certification regime we envision would be primarily administered by the private sector, we seek comment on whether the Commission should retain the ability to guide the development of the program through its continued review of the general security objectives. Additionally, we seek comment whether as part of its oversight authority, the Commission 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, we seek 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?[28]

27. Finally, it is possible that similar certification-related programs have already been implemented in the private sector.[29] 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

[27] *See 2000 Biennial Regulatory Review of Part 68 of the Commission's Rules*, CC Dkt. No. 99-216 *Report & Order* FCC 00-400 (rel. December 20, 2000) ¶¶ 20-24 . (*Part 68 Order*).

[28] *Cf. Part 68 Order*, ¶ 69 (noting that Commission will, at request of aggrieved party, conduct *de novo* review of technical criteria adopted by independent standards development organization).

[29] For example, pursuant to National Security Telecommunications and Information Systems Directive No. 501, the National Security Agency and other entities require certification of communication and ICT devices and personnel against standards for Information Security (NSA's CNSS 4011 Federal Security Certification and Training Standards, 4013A training standard for system administrators in federal departments and agencies, etc.). Cisco and other private vendors provide INFOsec certifications that satisfy these requirements. Additionally, entities such as the US-CERT's Control Systems Security Program (CSSP) seek to reduce the risks of cyber attack to "industrial control systems" and provides standards and references on topics that include the areas of our proposed security objectives for the certification program.

international? If so, which organizations should be considered and which specific points of alignment are relevant?

F. Security Criteria

28. As noted above, we envision that participating communications service providers would be assessed based on a stringent set of criteria. We seek 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? We observe 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?

29. We seek comment on possible criteria by which participating network operators would be assessed. We believe 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. We seek comment on this view.

30. We also seek 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 we 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.[30] 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 have been taken to avert MAC spoofing, enhance detection of it, and take effective corrective action once detected?

31. As Americans increasingly rely on broadband technology and IP-enabled services in their every day 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

[30] Broadband services, including cable modem service, include routers that serve as the ingress/regress point for user access to the Internet. The routers themselves each have a unique MAC address, which is an alpha-numeric code developed pursuant to the Ethernet standard. A popular method of controlling which computers have access to particular routers is to program into the routers the MAC addresses of the approved computers' network interface cards (NICs). The NICs are either plugged into one of the computer's ports or installed internally. Any non-programmed MAC addresses will be denied access. MAC spoofing allows the cyber hacker to either program the broadband service's routers with his/her MAC address to gain unauthorized Internet access, or to "sniff and steal" a MAC address already programmed into the router, for Internet access.

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.

32. 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, we seek 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?

33. We seek 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. We seek comment on how this should occur.

G. Structure of Security Regime

34. *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, we believe that it should be fairly balanced in terms of the points of view and industry segments that sit on it. Accordingly, we seek 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. We seek comment on whether any other potentially interested groups or entities should also be involved.

35. We recognize that a body representing so many diverse interests runs the risk of growing too large to be able to function effectively. Accordingly, we seek 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. We also seek 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).[31]

36. Assuming a certification authority possessed the significant degree of autonomy on which we seek 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?

37. *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, we seek 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*

[31] Detailed explanation of International Standard ISO/IEC 17011(E), sections 4.2 (Structure) and 4.3 (Impartiality).

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.[32] These ANSI procedures offer an array of due process protections. We seek comment on whether these decision-making requirements and/or any others should apply to the operations of the certification authority:

i. 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.

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

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

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

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

vi. 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.

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

viii. 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.

ix. International standards shall be taken into consideration.

x. 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.

38. We also seek 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?[33]

[32] *Part 68 Order*,. ¶¶ 28-29.

[33] The Commission has previously discussed the distinctions between the Organization Method and the Standards Committee Method. *See Part 68 Order*, ¶ 28. The first is typically used by associations that have, among their other activities, an interest in developing standards. The Standards Committee Method is most often used when a standard affects a broad range of diverse interests or where multiple associations or societies with similar interests (continued....)

39. As noted above, we seek 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? We seek comment on this aspect of the proposal.

1. Auditor Accreditation

40. As set out above, stringent, objective assessments of individual providers would compose an important part of the cyber security certification program on which we seek 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 we propose today? Should the Commission delegate the precise details about the structure of the accreditation process to an accreditation body? We anticipate, 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. We seek comment on the foregoing aspects of the program. Should we impose requirements on the auditor accreditation process to ensure competence, integrity and objectivity in the accreditation of auditors? If not, why should we choose not to impose such requirements? In addition, should we impose these requirements for auditor qualification in the application or approval process? Should we require that a certain number of auditors be accredited before the assessment or accreditation process may begin? Additionally, we seek 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.[34]

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

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

2. Development of Assessment Standards

43. It would, of course, be necessary to develop assessment standards to guide the auditors' review of the cyber security measures of participating providers. As we have indicated above, we seek comment about whether the network-security criteria will be definitive and objectively measurable. We

(Continued from previous page)
exist. The main difference between the two methods is that, in the Standards Committee method, ANSI generally requires the entity to be divided into a consensus body and a secretariat. The functions of the secretariat include overseeing the consensus body's compliance with ANSI criteria and administrative functions in connection with the development of standards. *Id.*

[34] ISO/IEC 17011(E), Conformity Assessment – General Requirements for Accreditation Bodies Accrediting Conformity Assessment Bodies (ISO 2005) (corrected version).

have 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, we seek 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."

44. 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. We seek 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? We believe 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? We seek comment to these questions.

45. 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, we seek comment on the appropriate composition of such a body. Again, in light of the narrow focus of such a body, we expect that it 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?

46. 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 that we discuss above in connection with the certification authority?

47. 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, we also seek comment on how frequently and through what mechanism the assessment procedures should be updated.

3. Maintaining Assessment Results; Conferring Security Certificate.

48. The final aspect of the network security program that we propose today 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 notice 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? We seek 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.[35] 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? We seek comment on whether we 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.

49. 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?

H. Appeals to the Commission

50. Although we have sought comment on a cyber security certification program as being largely a private sector process, we also seek 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? We seek comment on this aspect of the proposed program and the time periods that would be appropriate.

I. Security Certificate

51. 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? We recognize that communications technology and threats to cyber security are constantly evolving. Accordingly, we are 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, we acknowledge 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? We seek comment on this issue.

[35] We do not anticipate that certification will be a one-time event. Rather, to retain certification status, it will be necessary for communications providers to periodically resubmit to audit procedures to demonstrate their continuing compliance with applicable standards.

52. A related issue on which we seek comment is the appropriate renewal process for the security certification. We seek comment on whether the initial assessment of a provider's network security practices will be relatively extensive. We seek 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 we 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?

53. We also seek comment on the permissible uses by providers of the security certification. As we have discussed above, we envision 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?

54. We seek comment on what form the evidence of the security certificate should take. We presently expect that the Commission 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, we seek comment on the appropriate phrasing.

J. Enforcement Matters

55. We seek 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, we seek 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?

56. We expect that it would be unnecessary for the Commission to have a separate enforcement process for the auditors in a cyber security certification program. Rather, we expect 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. We seek comment on this question. Is it necessary for the Commission to create any other mechanisms relating to dispute resolution specific to this program?

57. 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 we 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? We seek comment on these questions and on other actions the Commission can take in this area.

K. Domestic and International Coordination

58. We recognize 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. We seek comment on cyber security efforts underway for these interconnected networks that could inform the certification program, as well as ways we might wish to coordinate, if at all, the development of our certification program, if any, with firms and agencies related to these networks. We also recognize 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). We invite 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.

L. Other Cyber Security Incentives

59. Apart from the issue of a certification program, we seek 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. We are interested not only in actions the Commission can take on its own, but also ideas that the Commission might recommend to its Federal partners or to Congress, if any. We also seek comment on how to improve education on cyber security issues. What actions, if any, can we 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 we better educate the industry about best practices and other methods to enhance cyber security in their communications networks and systems, if at all?

60. We further note 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.[36] Therefore, we seek comment on steps that

[36] Broadband services, including cable modem service, include routers that serve as the ingress/regress point for user access to the Internet. The routers themselves each have a unique MAC address, which is an alpha-numeric code developed pursuant to the Ethernet standard. A popular method of controlling which computers have access to particular routers is to program into the routers the MAC addresses of the approved computers' network interface cards (NICs). The NICs are either plugged into one of the computer's ports or installed internally. Any non-programmed MAC addresses will be denied access. MAC spoofing allows the cyber hacker to either program the broadband service's routers with his/her MAC address to gain unauthorized Internet access, or to "sniff and steal" a MAC address already programmed into the router, for Internet access.

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.

IV. PROCEDURAL MATTERS

A. Ex Parte Presentations

61. This matter will be treated as a "permit-but-disclose" proceeding in accordance with the Commission's *ex parte* rules.[37] 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.[38] Other rules pertaining to oral and written *ex parte* presentations in permit-but-disclose proceedings are set forth in section 1.1206(b) of the Commission's rules, 47 C.F.R. § 1.1206(b).

B. Comment Filing Procedures

62. Pursuant to sections 1.415, 1.419 and 1.430 of the Commission's rules, 47 CFR §§ 1.415, 1.419, 1.430, interested parties may file comments and reply comments on or before the dates indicated on the first page of this document. Comments may be filed using: (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).

- Electronic Filers: 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.

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

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

  - 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.

[37] *See* 47 C.F.R. §§ 1.1200 & 1.1206. Although a Notice of Inquiry proceeding is generally exempt from the *ex parte* rules, we find that the public interest is best served by treating this critical cyber security matter as a "permit-but-disclose" proceeding. *See* 47 C.F.R. §§1.1200(a), 1.1204(b)(1).

[38] *See* 47 C.F.R. § 1.1206(b).

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

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

C. Accessible Formats

63. 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).

V. ORDERING CLAUSE

64. 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

STATEMENT OF CHAIRMAN JULIUS GENACHOWSKI

Re: *In the Matter of a Cyber Security Certification Program, Notice of Inquiry,* PS Docket No. 10-93

More and more of our Nation's daily business depends on our broadband communications infrastructure. Companies large and small, and in every sector of the economy, including hospitals and other health care facilities, increasingly rely on communications networks to do their daily work. But for communications networks to remain a platform for global opportunity and prosperity, it is essential that end users of all types – consumers, and businesses large and small – remain confident that our global networks are safe and secure.

Increasingly, however, our communications networks are under attack. Viruses, denial of service attacks, harmful spam, and a host of other threats challenge end users and network operators. To ensure that consumers and businesses are fully protected from attacks that affect or occur over the communications infrastructure, the National Broadband Plan recommended that the Commission initiate a proceeding to establish a cyber security certification program and other incentive programs. The goal is to create incentives for broadband communications service providers to upgrade their cyber security measures.

This Notice of Inquiry represents an initial and necessary step to implementing this recommendation and enhancing the cyber security of our Nation's communications systems.

STATEMENT OF COMMISSIONER MICHAEL J. COPPS

Re: *In the Matter of a Cyber Security Certification Program, Notice of Inquiry*, PS Docket No. 10-93

Job One of the FCC is the security of this nation's infrastructure. That security has many ramifications—human lives and safety, of course, but also the economic, governmental and social functioning of the entire country. President Obama has rightly made protecting this infrastructure from cyber attacks a top national security priority. As the President has said, we must be ready to "deter, prevent, detect and defend against attacks and recover quickly from any disruptions or damage." The Administration's *Cyberspace Policy Review*, in which the FCC participated, recognizes the importance of the public sector and the private sector working together to ensure that the market delivers more secure products and services for the American people. Today, based on recommendations from the National Broadband Plan, we start to examine incentives programs to do just this.

I commend the Chairman and the Public Safety and Homeland Security Bureau for moving forward with the concept of a cyber security certification program. I welcome—and earnestly solicit—the thoughts and the comments of outside experts in the field of cyber security, and I encourage all other concerned stakeholders to contribute their input too. Cyber security, after all, affects us all. It is my hope that such a stamp-of-approval program will foster stronger security for this nation's network infrastructure and provide users with more information about their providers' security practices.

STATEMENT OF COMMISSIONER ROBERT M. McDOWELL

Re: *In the Matter of a Cyber Security Certification Program, Notice of Inquiry*, PS Docket No. 10-93

In light of America's increasing dependence on broadband communications services and given trends suggesting an increased susceptibility to operator error and malicious cyber attacks, efforts to promote greater vigilance among market participants, increase the security of our communications infrastructure and offer more information about cyber security practices would benefit consumers of broadband services. If consumers receive adequate information – the knowledge about the tools and techniques used by their service provider to combat criminals and hackers – they will no doubt be more comfortable with their broadband experience.

As always, I look forward to engaging with industry and interested parties to learn more about the work being undertaken in this area. Thank you to Jamie Barnett and your entire team. This is critically important and I appreciate the work you are doing.

STATEMENT OF COMMISSIONER MIGNON L. CLYBURN

Re: *In the Matter of a Cyber Security Certification Program, Notice of Inquiry,* PS Docket No. 10-93

Our Nation's economic prosperity depends on increased deployment and adoption of broadband services; but that prosperity, as well as the safety and security of our Nation's citizens, will be compromised if our broadband networks are not secure. When you consider that our Nation's networks have become more susceptible to cyber crime, and that $7 trillion worth of transactions – half of our Nation's Gross Domestic Product for 2009 -- moves over communications networks, it is plain that we must take immediate action to enhance our cyber security.

I was very pleased to see the urgency that the National Broadband Plan placed on developing a national cyber security strategy within 180 days. I am even more encouraged by the Commission adopting this *Notice of Inquiry on the Cyber Security Certification Program* in our first open meeting after announcing the Plan. By moving so quickly to enhance our Nation's cyber security, the Commission places the security and safety interests of our Nation's citizens at the head of the line – exactly where they should be.

This Notice of Inquiry takes a prudent, careful, and comprehensive approach, to determining the best methods to encourage communications service providers to implement best practices in cyber security. As recently as November 2009, the National Security Agency estimated that as much as 80 percent of cyber crime could be prevented by simply instituting proper configuration policies and conducting good network monitoring. One solution is to ensure that cyber security best practices are being implemented. Therefore, I believe the item wisely recommends a certification program that can efficiently enhance the development of the proper network objectives and technical criteria for achieving the most secure communications networks; ensure accurate information about the extent to which service providers are implementing cyber security best practices; and create the proper incentives for small and large service providers to voluntarily adopt these best practices.

I applaud the Public Safety and Homeland Security Bureau for its excellent work in crafting this Notice of Inquiry.

STATEMENT OF COMMISSIONER MEREDITH ATTWELL BAKER

Re: *In the Matter of a Cyber Security Certification Program, Notice of Inquiry*, PS Docket No. 10-93

I am pleased the prominence we are giving cyber security as we begin implementation of the National Broadband Plan. One of the core challenges of the broadband world is how do we safeguard and protect our networks and data from cyber security threats. We are faced by a troubling trend of escalating efforts – both organized and individual – to destroy, steal, harm or alter online data and networks. If online content is not safe, the promise of the National Broadband Plan to enable substantial advancements in business, energy, health care, and education will not be achieved.

As we proceed, my hope is our consideration of these issues track closely with the recommendations and work of our recently chartered Communications Security, Reliability, and Interoperability Council (CSRIC), and any decisions are made in close coordination with other governmental efforts, particularly those of the Department of Homeland Security. We should ensure our actions do not add additional layers of requirements or duplicative obligations on providers. Further, any Commission action – whether mandatory or voluntary – must ensure that network operators retain the flexibility and adaptability to respond to evolving cybersecurity threats and to innovate in their network operations.