DEPARTMENT OF COMMERCE

Office of the Secretary

National Institute of Standards and Technology

International Trade Administration

National Telecommunications and Information Administration

[Docket No. 110527305–1303–02]

Cybersecurity, Innovation, and the Internet Economy

AGENCY: Office of the Secretary, National Institute of Standards and Technology, International Trade Administration, and National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice and Request for Public Comments.

SUMMARY: The Department of Commerce's (Department) Internet Policy Task Force is conducting a comprehensive review of the nexus between cybersecurity and innovation in the Internet economy. On July 28, 2010, the Department published a Notice of Inquiry seeking comment from all Internet stakeholders on the impact of cybersecurity policy issues in the United States and around the world on the pace of innovation in the information economy. The Department now seeks further comment on its report entitled, ''Cybersecurity, Innovation and the Internet Economy,'' available at *http://www.nist.gov/itl.* Through this Notice requesting comments on the report, the Department hopes to spur further discussion with Internet stakeholders that will lead to the development of a series of Administration positions that will help develop an action plan in this important area.

DATES: Comments are due on or before 11:59 p.m. on August 1, 2011.

ADDRESSES: Comments will be accepted by e-mail only. Comments should be sent to *SecurityGreenPaper@nist.gov* with the subject line ''Comments on Cybersecurity Green Paper.'' Comments will be posted at *http://www.ntia.doc.gov/internetpolicytaskforce/.*

FOR FURTHER INFORMATION CONTACT: Jon Boyens, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 893, Gaithersburg, MD 20819, *jon.boyens@nist.gov.* Please direct media inquires to NIST's Office of Public Affairs at (301) 975–NIST.

SUPPLEMENTARY INFORMATION: Over the past two decades, the Internet has become increasingly important to fueling the Nation's economic competitiveness, to promoting innovation, and to enhancing our collective well-being. As the Internet continues to grow in all aspects of our lives, the parallel issue of cybersecurity risks continues to increase and evolve.

Today's cybersecurity threats include indiscriminate and broad-based attacks designed to exploit the interconnectedness of the Internet. Increasingly, the threats also involve targeted attacks, the purpose of which is to steal, manipulate, destroy or deny access to sensitive data, or to disrupt computing systems. These threats are exacerbated by the interconnected and interdependent architecture of today's computing environment. Theoretically, security deficiencies in one area may provide opportunities for exploitation elsewhere.

Despite increasing awareness of the associated risks, broad swaths of the economy and individual actors, ranging from consumers to large businesses, do not take advantage of available technology and processes to secure their systems, and protective measures are not evolving as quickly as the threats. This general lack of investment puts firms and consumers at greater risk, leading to economic loss at the individual and aggregate levels and poses a threat to national security.

President Obama's *Cyberspace Policy Review* in May 2009 articulated the many reasons government must work closely with the private sector and other partners to address these risks. As stated in the *Review,* ''information and communications networks are largely owned and operated by the private sector, both nationally and internationally. Thus, addressing network security issues requires a public-private partnership as well as international cooperation and norms.''

In addition, the Administration has promoted cybersecurity legislation that would catalyze the development of norms for practices of entities that maintain our critical infrastructure. These entities include sectors such as energy, critical manufacturing, and emergency services whose disruption would have a debilitating impact on individual security, national economic security, national public health and safety. The proposed legislation requires these entities to develop a baseline framework of protection based on risk—a function of threat, vulnerability, and consequences. The Department of Homeland Security (DHS), in coordination with sector-specific agencies and other relevant departments, would promulgate the list of covered entities using the established criteria and input from the Federal Government, state and local governments, and the private sector.

The U.S. Department of Commerce (Department) has focused its efforts on developing public policies and private sector norms whose voluntary adoption could improve the overall cybersecurity posture of private sector infrastructure operators, software and service providers, and users outside the critical infrastructure. Entities in these areas have not been the main focus of cybersecurity activities to date, yet they can be at great risk—and can put others at great risk—if they do not adequately secure their networks and services. Yet, attempting to develop policies to protect each industry with equal weight, regardless of criticality, will lead to placing too much emphasis on lesser concerns. We must instead find the right protections for each sector and sub-sector and promote the right policies to get them implemented.

In early 2010, the Department launched the Internet Policy Task Force (Task Force), charged with addressing the Internet's most pressing policy issues and with recommending new policies. After several months of consultations with stakeholders, the Task Force published a Notice of Inquiry (NOI) and convened a symposium on Cybersecurity, Innovation, and the Internet Economy leading to this preliminary set of recommendations in the Green Paper entitled ''Cybersecurity, Innovation, and the Internet Economy''.[1] In this paper, the Task Force asks many follow-up questions to gain additional feedback and to help the Department determine how to proceed. The goal of this undertaking is to ensure that the Task Force is on the right course with its recommendations and to identify technical and policy measures that might close the gap between today's status quo and reasonably achievable levels of cyber-protection outside of critical infrastructure sectors. The Green Paper will also serve as a vehicle to spur further discussion with Internet stakeholders on this important area of policy development.

In particular, many responses to the 2010 NOI highlighted a large group of functions and services that should be the subject of our efforts. The Task Force is calling this group the ''Internet and Information Innovation Sector'' (I3S). The I3S includes functions and

[1] The text of the Green Paper is available at *http://www.nist.gov/itl.*

services that create or utilize the Internet or networking services and have large potential for growth, entrepreneurship, and vitalization of the economy, but would fall outside the classification of covered critical infrastructure as defined by existing law and Administration policy. Business models may differ, but the following functions and services are included in the I3S:

- Provision of information services and content;
- Facilitation of the wide variety of transactional services available through the Internet as an intermediary;
- Storage and hosting of publicly accessible content; and
- Support of users' access to content or transaction activities, including, but not limited to application, browser, social network, and search providers.

The I3S is comprised of companies, from small businesses to ''brick and mortar-based firms'' with online services to large companies that only exist on the Internet. These companies are significantly impacted by cybersecurity concerns, yet do not have the same level of operational criticality that would cause them to be designated as covered critical infrastructure. The Task Force supports efforts to increase the security posture of I3S services and functions from cybersecurity risks without regulating these services as covered critical infrastructure. A primary goal of this Green Paper is to spark a discussion of the scope of this newly defined sector and the policies needed to protect it independently of, but in concert with, the discussion on protections within the critical infrastructure.

Request for Information

Request for Comment: This Notice seeks input on the report ''Cybersecurity, Innovation, and the Internet Economy'' (*http://www.nist.gov/itl*). The questions below, which also appear in Appendix A of the report, are intended to assist in identifying issues. They should not be construed as a limitation on comments that parties may submit. Comments that contain references to studies, research and other empirical data that are not widely published should include copies of the referenced materials with the submitted comments.

1. How should the Internet and Information Innovation Sector (I3S) be defined? What kinds of entities should be included or excluded? How can its functions and services be clearly distinguished from critical infrastructure?

2. Is the Department of Commerce's focus on an I3S the right one to target the most serious cybersecurity threats to the Nation's economic and social well-being related to non-critical infrastructure?

3. What are the most serious cybersecurity threats facing the I3S as currently defined?

4. Are there other sectors not considered critical infrastructure where similar approaches might be appropriate?

5. Should I3S companies that also offer functions and services to covered critical infrastructure be treated differently than other members of the I3S?

6. Are there existing codes of conduct that the I3S can utilize that adequately address these issues?

7. Are there existing overarching security principles on which to base codes of conduct?

8. What is the best way to solicit and incorporate the views of small and medium businesses into the process to develop codes?

9. What is the best way to solicit and incorporate the views of consumers and civil society?

10. How should the U.S. Government work internationally to advance codes of conduct in ways that are consistent with and/or influence and improve global norms and practices?

11. Are the standards, practices, and guidelines indicated in section III, A, 2 and detailed in Appendix B of the Green Paper appropriate to consider as keystone efforts? Are there others not listed in the Green Paper that should be included?

12. Is there a level of consensus today around all or any of these guidelines, practices, and standards as having the ability to improve security? If not, is it possible to achieve consensus? If so, how?

13. What process should the Department of Commerce use to work with industry and other stakeholders to identify best practices, guidelines, and standards in the future?

14. Should efforts be taken to better promote and/or support the adoption of these standards, practices, and guidelines?

15. In what way should these standards, practices, and guidelines be promoted and through what mechanisms?

16. What incentives are there to ensure that standards are robust? What incentives are there to ensure that best practices and standards, once adopted, are updated in light of changing threats and new business models?

17. Should the government play an active role in promoting these standards, practices, and guidelines? If so, in which areas should the government play more of a leading role? What should this role be?

18. How can automated security be improved?

19. What areas of research in automation should be prioritized and why?

20. How can the Department of Commerce, working with its partners, better promote automated sharing of threat and related signature information with the I3S?

21. Are there other examples of automated security that should be promoted?

22. What conformance-based assurance programs, in government or the private sector need to be harmonized?

23. In a fast changing and evolving security threat environment, how can security efforts be determined to be relevant and effective? What are the best means to review procedural improvements to security assurance and compliance for capability to pace with technological changes that impact the I3S and other sectors?

24. What are the right incentives to gain adoption of best practices? What are the right incentives to ensure that the voluntary codes of conduct that develop from best practices are sufficiently robust? What are the right incentives to ensure that codes of conduct, once introduced, are updated promptly to address evolving threats and other changes in the security environment?

25. How can the Department of Commerce or other government agencies encourage I3S subsectors to build appropriate best practices?

26. How can liability structures and insurance be used as incentives to protect the I3S?

27. What other market tools are available to encourage cybersecurity best practices?

28. Should Federal procurement play any role in creating incentives for the I3S? If so, how? If not, why not?

29. How important is the role of disclosure of security practices in protecting the I3S? Will it have a significant financial or operational impact?

30. Should an entity's customers, patients, clients, etc. receive information regarding the entity's compliance with certain standards and codes of conduct?

31. Would it be more appropriate for some types of companies within the I3S to be required to create security plans

and disclose them to a government agency or to the public? If so, should such disclosure be limited to where I3S services or functions impact certain areas of the covered critical infrastructure?

32. What role can the Department of Commerce play in promoting public-private partnerships?

33. How can public-private partnerships be used to foster better incentives within the I3S?

34. How can existing public-private partnerships be improved?

35. What are the barriers to information sharing between the I3S and government agencies with cybersecurity authorities and among I3S entities? How can they be overcome?

36. Do current liability structures create a disincentive to participate in information sharing or other best practice efforts?

37. What is the best means to promote research on cost/benefit analyses for I3S security?

38. Are there any examples of new research on cost/benefit analyses of I3S security? In particular, has any of this research significantly changed the understanding of cybersecurity and cybersecurity related decision-making?

39. What information is needed to build better cost/benefit analyses?

40. What new or increased efforts should the Department of Commerce undertake to facilitate cybersecurity education?

41. What are the specific areas on which education and research should focus?

42. What is the best way to engage stakeholders in public/private partnerships that facilitate cybersecurity education and research?

43. What areas of research are most crucial for the I3S? In particular, what R&D efforts could be used to help the supply chain for I3S and for small and medium-sized businesses?

44. What role does the move to cloud-based services have on education and research efforts in the I3S?

45. What is needed to help inform I3S in the face of a particular cyber threat? Does the I3S need its own ''fire department services'' to help address particular problems, respond to threats, and promote prevention or do enough such bodies already exist?

46. What role should Department of Commerce play in promoting greater R&D that would go above and beyond current efforts aimed at research, development, and standards?

47. How can the Department of Commerce work with other Federal agencies to better cooperate, coordinate, and promote the adoption and development of cybersecurity standards and policy internationally?

Dated: June 9, 2011.

Gary Locke,

Secretary of Commerce.

Patrick Gallagher,

Under Secretary of Commerce for Standards and Technology.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information.

Francisco J. Sánchez,

Under Secretary of Commerce for International Trade.

[FR Doc. 2011–14710 Filed 6–14–11; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XA493

Marine Fisheries Advisory Committee Meeting

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice of open public meeting.

SUMMARY: This notice sets forth the schedule and proposed agenda of a forthcoming meeting of the Marine Fisheries Advisory Committee (MAFAC). The members will discuss and provide advice on issues outlined under **SUPPLEMENTARY INFORMATION** below.

DATES: The meeting is scheduled for June 27, 2011, 3–4:30 p.m., Eastern Daylight Time.

ADDRESSES: Conference call. Public access is available at SSMC3, Room 14400, 1315 East-West Highway, Silver Spring, MD 20910.

FOR FURTHER INFORMATION CONTACT: Mark Holliday, MAFAC Executive Director; (301) 713–2239 x-120; e-mail: *Mark.Holliday@noaa.gov.*

SUPPLEMENTARY INFORMATION: As required by section 10(a)(2) of the Federal Advisory Committee Act, 5 U.S.C. App. 2, notice is hereby given of a meeting of MAFAC. The MAFAC was established by the Secretary of Commerce (Secretary), and, since 1971, advises the Secretary on all living marine resource matters that are the responsibility of the Department of Commerce. The complete charter and summaries of prior meetings are located online at *http://www.nmfs.noaa.gov/ocs/mafac/.*

Matters To Be Considered

This agenda is subject to change.

The meeting is convened to discuss policies and guidance on National Ocean Policy Strategic Action Plans.

Special Accommodations

These meetings are physically accessible to people with disabilities. Requests for sign language interpretation or other auxiliary aids should be directed to Mark Holliday, MAFAC Executive Director; (301) 713–2239 x 120 by May13, 2011.

Dated: June 10, 2011.

Eric C. Schwaab,

Assistant Administrator for Fisheries, National Marine Fisheries Service.

[FR Doc. 2011–14845 Filed 6–10–11; 4:15 pm]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XA494

Endangered Species; File No. 10027

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Notice; receipt of application for a permit modification.

SUMMARY: Notice is hereby given that the Center for Biodiversity and Conservation, American Museum of Natural History (Responsible Party: Eleanor Sterling, PhD), Central Park West at 79th Street, New York, New York 10024, has requested a modification to scientific research Permit No. 10027.

DATES: Written, telefaxed, or e-mail comments must be received on or before July 15, 2011.

ADDRESSES: The modification request and related documents are available for review by selecting ''Records Open for Public Comment'' from the Features box on the Applications and Permits for Protected Species (APPS) home page, *https://apps.nmfs.noaa.gov/,* and then selecting File No. 10027–05 from the list of available applications. These documents are also available upon written request or by appointment in the following offices:

Permits, Conservation and Education Division, Office of Protected Resources, NMFS, 1315 East-West Highway, Room 13705, Silver Spring, MD 20910; phone (301) 713–2289; fax (301) 713–0376; and

Pacific Islands Region, NMFS, 1601 Kapiolani Blvd., Rm 1110, Honolulu, HI