Affairs Coordinator, telephone: 781–545–8026, ext. 206.

SUPPLEMENTARY INFORMATION: The Council was established in March 2001 to assure continued public participation in the management of the Sanctuary. The Council's 23 members represent a variety of local user groups, as well as the general public, plus seven local, state and Federal government agencies. Since its establishment, the Council has played a vital role in advising NOAA on critical issues and is currently focused on the sanctuary's final five-year Management Plan.

The Stellwagen Bank National Marine Sanctuary encompasses 842 square miles of ocean, stretching between Cape Ann and Cape Cod. Renowned for its scenic beauty and remarkable productivity, the sanctuary supports a rich diversity of marine life including 22 species of marine mammals, more than 30 species of seabirds, over 60 species of fishes, and hundreds of marine invertebrates and plants.

Authority: 16 U.S.C. 1431, *et seq.*

(Federal Domestic Assistance Catalog Number 11.429 Marine Sanctuary Program)

Dated: July 21, 2010.

Daniel J. Basta,

Director, Office of National Marine Sanctuaries, National Ocean Service, National Oceanic and Atmospheric Administration.

[FR Doc. 2010–18300 Filed 7–27–10; 8:45 am]

BILLING CODE 3510–NK–M

DEPARTMENT OF COMMERCE

Office of the Secretary

National Institute of Standards and Technology

International Trade Administration

National Telecommunications and Information Administration

[Docket No.: 100721305–0305–01]

Cybersecurity, Innovation and the Internet Economy

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

ACTION: Notice of inquiry.

SUMMARY: The Department of Commerce's Internet Policy Task Force is conducting a comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy. The Department seeks comments from all stakeholders, including the commercial, academic and civil society sectors, on measures to improve cybersecurity while sustaining innovation. Preserving innovation, as well as private sector and consumer confidence in the security of the Internet economy, are important for promoting economic prosperity and social well-being overall. In particular, the Department seeks to develop an up-to-date understanding of the current public policy and operational challenges affecting cybersecurity, as those challenges may shape the future direction of the Internet and its commercial use, both domestically and globally. After analyzing comments on this Notice, the Department intends to issue a report that will contribute to the Administration's domestic and international policies and activities in advancing both cybersecurity and the Internet economy.

DATES: Comments are due on or before September 13, 2010.

ADDRESSES: Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Submissions may be in any of the following formats: HTML, ASCII, Word, rtf, or pdf. Online submissions in electronic form may be sent to *cybertaskforce@doc.gov.* Paper submissions should include a three and one-half inch computer diskette or compact disc (CD). Diskettes or CDs should be labeled with the name and organizational affiliation of the filer and the name of the word processing program used to create the document. Comments will be posted at *http://www.ntia.doc.gov/internetpolicytaskforce* and *http://csrc.nist.gov.*

FOR FURTHER INFORMATION CONTACT: For questions about this Notice contact: Jon Boyens, International Trade Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW., Room 2806, Washington, DC 20230, telephone (202) 482–0573, e-mail *Jon.Boyens@trade.gov;* or Alfred Lee, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue, NW., Room 4725, Washington, DC 20230, telephone (202) 482–1880, e-mail *Alee@ntia.doc.gov.* Please direct media inquires to the National Institute of Standards and Technology's Office of Public and Business Affairs at (301) 975–6478.

SUPPLEMENTARY INFORMATION: The Internet has become vitally important to U.S. innovation, prosperity, education, civic activity and cultural life as well as aspects of our national security. A top priority of the Department of Commerce is to ensure that the Internet remains an open and trusted infrastructure, both for commercial entities and individuals. In pursuit of this priority, the Department has created an Internet Policy Task Force whose mission is to identify leading policy challenges and to recommend possible solutions. The Task Force leverages expertise across many bureaus at the Department, including those responsible for cybersecurity standards and best practices, information and communications policy, international trade, intellectual property, business advocacy and export control. This Notice of Inquiry is one in a series of inquiries from the Task Force. Other reviews examine information privacy, global free flow of information on the Internet, and online copyright protection issues. The Task Force may explore additional areas in the future.

The Task Force's cybersecurity work aims to identify public policies and private-sector norms that can: (1) Promote conduct by firms and consumers that collectively will sustain growth in the Internet economy and improve the level of security of the infrastructure and online environment that support it; (2) enhance individual and collaborative efforts by those actors who are in the best position to assist firms and their customers in addressing cybersecurity challenges; (3) improve the ability of firms and consumers to keep pace with ever-evolving cybersecurity risks; and (4) promote individual privacy and civil liberties. Public policies and private-sector practices that promote innovation and enhance cybersecurity will help assure that the Internet remains fertile ground for an expanding range of beneficial commercial and consumer activity.

Internet Growth and Evolving Cybersecurity Challenges: The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data. At the same time that businesses and consumers rely more and more on such capabilities, cybersecurity risks continue to plague the Internet economy, and it seems highly unlikely that all risks will ever be completely eliminated.

Sources of cybersecurity risks include individual criminals, organized crime, terrorists, and nation-states. Cyber intrusions and attacks are mounted against commercial and individual users, as well as against government, military, and critical infrastructure networks (*e.g.,* energy, water, sewage, transportation, banking, and financial networks). These intrusions and attacks often seek to steal, manipulate, destroy, or deny access to sensitive data and sometimes attempt to disable or disrupt individual systems.[1] Media outlets regularly report on the activities of those who disseminate viruses, spyware, and other malware, as well as those who spoof e-mail addresses, distribute spam, phish for sensitive personal information, and create botnets.[2] Cyber threats can originate from anywhere in the world. They not only target computers, but also mobile phones and other devices connected to the Internet.

Cybersecurity risks seem to evolve as rapidly as the Internet expands, and those risks are becoming increasingly global in nature. Keeping pace with cybersecurity risks requires all users, even the most sophisticated users, to be aware of the threats and improve upon their security practices on an ongoing basis. Creating incentives to motivate all parties in the Internet economy to make appropriate security investments in response to risks they face requires a careful balance of technical and public policy measures.

The constantly evolving nature of the threats and vulnerabilities not only affects individual firms and their customers, but collectively the threats pose a persistent economic and national security challenge. Computing devices are highly and increasingly interconnected, meaning that security deficiencies in a limited number of systems can be exploited to launch cyber intrusions or attacks on other systems. Put another way, poor cyber "hygiene" on one Internet-connected computer negatively impacts other connected computers.

Given the breadth and importance of this challenge, government and private sector actors have for many years been pursuing a range of mitigation strategies. Currently at the Federal level, the White House's Cybersecurity Coordinator is responsible for setting a national agenda and for coordinating Executive Branch cybersecurity activities. Specific Federal activities in this area include research and training, threat reporting and analysis, information collection and dissemination, consumer awareness, and policy development. In addition, the Director of the Office of Management and Budget (OMB) is responsible for overseeing Federal agency information security policies and practices under the Federal Information Security Management Act of 2002.

The Department of Homeland Security (DHS) is an especially important Federal actor that serves as a focal point for the security of cyberspace. It provides consolidated intrusion detection, incident analysis and cyber response capabilities to protect Federal agencies' external access points, including access to the Internet. While the Department of Defense (DOD) defends military and national security systems, DHS has the lead in securing federal civilian systems. DHS also works with public and private stakeholders to protect critical infrastructure and key resources (CIKR).[3] A number of entities within the Department of Justice, including the Federal Bureau of Investigation, as well as the United States Secret Service in DHS, track and prosecute cyber crimes. The National Science and Technology Council and its Committee on Technology serve as the coordinating organization over the Networking and Information Technology Research and Development (NITRD) program, which is the primary mechanism by which the U.S. Government coordinates its unclassified networking and IT research and development investments, including cybersecurity research and development.[4]

The Department of Commerce has programs that complement and support these and other federal efforts. For example, the Department's National Institute of Standards and Technology (NIST) [5] develops standards and guides for securing non-national security Federal information systems. It defines minimum security requirements for federally held information and for information systems. NIST is also a primary contributor and member of the NITRD program, leading research and development in computer forensics tool testing, seamless mobility, trustworthy information systems, information security automation, combinatorial testing, next generation access control, and Internet infrastructure protection (with DHS funding). NIST also is responsible for the National Software Reference Library, National Vulnerability Database, and Security Content Automation Protocol. NIST identifies methods and metrics for assessing the effectiveness of security requirements; evaluates private sector security policies for potential federal agency use; and provides general cybersecurity technical support and assistance to the private sector and federal agencies. Moreover, over the

[1] *See, e.g., Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure,* May 29, 2009, at 1, *http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf* (Cyberspace Policy Review), *citing* Director of National Intelligence, *Annual Threat Assessment of the Intelligence Community for the Armed Services Committee, Statement for the Record,* March 10, 2009, at 39.

[2] *See, e.g., id.* at 2 (listing several examples of media reported incidents); *see also* David S. Wall, *Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime,* 22 International Review of Law, Computers and Technology 45 (2008). A botnet, short for robot network, is an aggregation of compromised computers that are taken over via network connections without the knowledge or consent of their owners. Michigan Information Sharing and Analysis Center, *Monthly Cyber Security Tips Newsletter* (September 2007), *http://www.michigan.gov/documents/cybersecurity/CSNewsletter_September2007_207450_7.pdf.*

[3] DHS oversees critical infrastructure protection, operates the United States Computer Emergency Readiness Team (US–CERT), oversees implementation of the Trusted Internet Connection initiative, and takes other actions to help secure both the federal civilian government systems and the private sector. DHS exercises primary responsibility within the executive branch for the operational aspects of Federal agency cybersecurity with respect to the Federal information systems that fall within the Federal Information Security Management Act of 2002 (FISMA). These responsibilities include overseeing the government-wide and agency-specific implementation of and reporting on cybersecurity policies and guidance; overseeing and assisting government-wide and agency-specific efforts to provide adequate, risk-based and cost-effective cybersecurity. Under FISMA, the Director of the Office of Management and Budget (OMB) oversees federal agency information security policies and practices, and OMB has directed all departments and agencies to coordinate and cooperate with DHS as necessary to carry out its FISMA responsibilities. OMB Memorandum M–10–28 Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and the Department of Homeland Security (DHS), *http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-28.pdf.*

[4] In addition, the Federal Communications Commission, an independent regulatory agency, is considering launching a voluntary certification program to encourage communications service providers to implement cybersecurity best practices. *See http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-63A1.pdf.*

[5] The 1965 Brooks Act gave the National Bureau of Standards (now NIST) responsibilities for federal information technology standards. Public Law 89–306 (Oct. 30, 1965). The Computer Security Act of 1987 reaffirmed the responsibilities of NIST for the security of unclassified, non-military government computer systems. Public Law. 100–235 (Jan. 8, 1988). Under the law, the role of the National Security Agency (NSA) was limited in the civilian security realm to providing technical assistance. The 2002 Cyber Security Research and Development Act authorized funding to NIST for computer and network security research and established status reporting requirements. Public Law 107–305 (Nov. 27, 2002). The 2002 Federal Information Security Management Act provided for development and maintenance by NIST of minimum controls required to protect federal information and information systems. Title III of Public Law 107–347 (Dec. 17, 2002).

past two decades, the Department's National Telecommunications and Information Administration (NTIA), in its role as principal adviser to the President on telecommunications and information policies, has worked closely with other parts of government on broadband deployment, Internet policy development, securing the Internet namespace, and other issues. As an advocate for our nation's businesses, NTIA has played an instrumental role in developing policies that have helped commerce over the Internet flourish.[6]

Through its Internet Policy Task Force, the Department intends to recommend public policies and private-sector norms that can markedly improve the overall cybersecurity posture of private sector infrastructure operators, software and service providers, and users outside the critical infrastructure and key resources realm and of their customers.

Cybersecurity and Commerce: Due to the Department's over-arching responsibility to advance the nation's commercial interests, the Task Force is focused on the cybersecurity challenges facing businesses and consumers that use the Internet.

The nation's e-commerce interests are significant. Growth in online sales and expanding use of the Internet are creating new jobs and contributing directly to our economic recovery. Businesses of all sizes increasingly use the Internet to order and track inventory, sell products and services, store financial and other proprietary information, and interact with their customers. These shifts in business practices and other measures have led to a greatly increased average growth in productivity over the last fifteen years.[7] Over the long term, such growth benefits our global competitiveness.[8]

Taking into account both business-to-consumer and business-to-business transactions, online commerce in 2007 accounted for more than $3 trillion in revenue for U.S. companies.[9] In the business-to-consumer e-commerce space, the United States economy enjoyed an increase in revenue of more than 500 percent between 1999 and 2007.[10] Even during the recent economic downturn, the economic benefits provided by the Internet economy increased. In 2009, online retail sales grew 2.0 percent to reach $134.9 billion,[11] while total retail sales fell 7 percent in that same year. Also in 2009, U.S. mobile commerce sales grew more than 200 percent compared to the previous year, reaching $1.2 billion.[12] Analysts expect this growth to continue in 2010, projecting $2.4 billion in mobile commerce.[13]

Notwithstanding this consistent, impressive growth, companies continue to face significant challenges in their ability to appropriately protect their computer systems, secure their proprietary, personal, and financial information, and safeguard the integrity of business and other transactions that they conduct over the Internet.

Reports of significant, persistent, individual cyber intrusions occur on a regular basis, as do reports of widespread, untargeted cyber incidents. The Cyberspace Policy Review described a coordinated attack in 49 cities on more than 130 automated teller machines in 2008, as well as a single 2007 data breach at one company that resulted in more than 45 million compromised consumer financial accounts.[14] While some cyber intrusions are highly sophisticated, some require relatively little skill or effort. For instance, criminals can use widely available, low cost "crimeware kits" to exploit computer systems and software vulnerabilities in order to launch malware against targeted computer systems.[15]

The financial cost of cyber threats to firms and their customers appears to be significant. Though current fraud losses attributed to cybersecurity data breaches are small in comparison to total annual business fraud losses, they are increasing, rising from 7 percent of total fraud losses in 2007 to 11 percent in 2008. In 2009, the dollar loss from all cases of online crime referred to law enforcement in the United States reached $550 million, more than twice the 2008 level.[16]

Small businesses have just as much reason to focus on cybersecurity as do larger enterprises yet they are less likely to have adequately protected themselves from their risks. According to a National Cybersecurity Alliance poll, 65 percent of small businesses store customer data online, 43 percent store financial records online, 33 percent store credit card information online, and 22 percent have intellectual property and other sensitive corporate content online.[17] The same poll shows that only 14 percent of these firms have anyone solely focused on information technology security; only 53 percent check their computers to ensure that anti-virus, anti-spyware, firewalls, and operating systems are up to date; 20 percent say that they use the minimum threshold of security to protect customer and employee data, but 42 percent believe that their customers are

[6] *See* 47 U.S.C. 902 (b)(2)(D) (providing that NTIA has "[t]he authority to serve as the President's principal adviser on telecommunications policies pertaining to the Nation's economic and technological advancement and to the regulation of the telecommunications industry"); *see also* Federal Communications Commission, *Connecting America: The National Broadband Plan,* at 55 (2010), *http://download.broadband.gov/plan/national-broadband-plan.pdf.* In 1993, the White House formed the Information Infrastructure Task Force (White House Task Force), chaired by the Secretary of Commerce, to develop telecommunications and information policies to promote the development of the Internet. In 1997, the White House Clinton Administration published *A Framework for Global Electronic Commerce.* This was the work of an interagency working group of high level representatives of several cabinet agencies, including the Departments of Treasury, State, Justice and Commerce, as well as the Executive Office of the President, including the Council of Economic Advisors, the National Security Council, the Office of Science and Technology Policy, the Office of the Vice President, and the U.S. Trade Representative. Independent commissions including the Federal Communications Commission and the Federal Trade Commission also contributed to the working group. In several instances, the *Framework* notes NTIA's collaborative efforts, in conjunction with other federal agencies, such as the State Department, Federal Trade Commission, U.S. Trade Representative, to explore opportunities for international cooperation to protect consumers and to prosecute false, deceptive, and fraudulent commercial practices in cyberspace. President William J. Clinton and Vice President Albert Gore, Jr., *A Framework for Global Electronic Commerce* (1997) (pagination not available), *http://clinton4.nara.gov/WH/New/Commerce/*; *see also* Memorandum on Electronic Commerce, 33 Weekly Comp. Pres. Doc 1006 (July 1, 1997).

[7] Executive Office of the President of the United States, *Economic Report of the President* (Feb. 2010), *available at http://www.whitehouse.gov/administration/eop/cea/economic-report-of-the-president.*

[8] The Nation relies increasingly on the Internet not only as a platform for commercial activities, but also as a vehicle for innovation, national competitiveness, and a tool for efficiency, transparency and accountability in government.

[9] U.S. Census Bureau, *E–Stats,* May 28, 2009, *http://www.census.gov/econ/estats/2007/2007reportfinal.pdf,* at 2.

[10] *Id.* More recent data released in May 2010 show that this trend continued in 2008. U.S. Census Bureau, *E–Stats,* May 27, 2010, *http://www.census.gov/econ/estats/2008/2008reportfinal.pdf.*

[11] U.S. Census Bureau, "Quarterly Retail E–Commerce Sales: 4th Quarter 2008," Feb. 16, 2010.

[12] *U.S. M–Commerce Sales to Hit $2.4 Billion This Year, ABI Research Says,* Internet Retailer, Feb. 16, 2010, *http://www.internetretailer.com/2010/02/16/u-s-m-commerce-sales-to-hit-2-4-billion-this-year-abi-researc.*

[13] *Id.*

[14] Cyberspace Policy Review at 2.

[15] *See, e.g.,* Tom Zeller, Jr., *Cyberthieves Silently Copy Your Passwords as You Type,* New York Times, Feb. 27, 2006, *available at http://www.nytimes.com/2006/02/27/technology/27hack.html.*

[16] *See* Internet Crime Complaint Center, *2009 Internet Crime Report, http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.*

[17] National Cyber Security Alliance, Symantec, and Zogby International; *2009 NCSA/Symantec Small Business Study,* Oct. 2009, *http://www.staysafeonline.org/files/2009SMBStudy/FullSMBStudy2009%20FINAL.pdf,* at 4.

concerned about the IT security of their business. Though many businesses are increasing their cybersecurity budgets, anecdotally, the Task Force has been told that there is a continuous requirement for IT managers to justify their expenditure of company resources on cybersecurity.

Given this state of affairs, the Task Force believes that public policies affecting cybersecurity on the Internet, as well as private sector norms (both good and bad), require a fresh look. The Task Force recognizes the valuable roles, responsibilities, and capabilities of the private sector in creating tools and strategies to mitigate cyber risks associated with the Internet. More broadly, over the past two decades, the nation has benefitted greatly from industry-led, Internet-driven innovation and growth, with those benefits reflected throughout the entire economy. That said, the persistence of the cybersecurity challenges compels the Department to seek a better understanding of both how those challenges are affecting U.S. businesses and citizens, as well as useful steps that can enhance the security of e-commerce. Small, medium, and large businesses, and consumers, will continue to increase their reliance on the Internet. As that reliance grows, the level of cybersecurity must increase as well.

Contribution of This NOI to the Internet Policy Task Force: Responses to this Notice will assist the Department's Internet Policy Task Force in preparing a report on cybersecurity, innovation and the Internet economy. The primary purposes of the report will be to identify and evaluate cybersecurity challenges facing commercial actors and consumers outside the critical infrastructure and key resources sectors to analyze various approaches to meet those challenges. The Department would also like to know how it can improve its execution of core cybersecurity responsibilities, including those supporting CIKR sectors and their customers. The Task Force's report may include options and recommendations for changes in public policy, as well as recommendations for voluntary steps that will enhance the commercial sector's and consumers' cybersecurity preparedness. The Task Force is hopeful that the dialogue launched here and the responses to this inquiry will contribute to Administration-wide policy positions and global cybersecurity strategy.

Request for Comment

The primary focus of this inquiry, as reflected above and in the questions listed below, is on enhancing the cybersecurity practices of commercial actors, consumers, and citizens outside the CIKR sectors. Activities involving government systems, other critical infrastructures and key resources receive attention from the Department of Homeland Security and other agencies. As such, they are not the main subject of this inquiry. The questions below are intended to help frame the issues and should not be construed as a limitation on comments that parties may submit. Comments containing references, studies, research, and other empirical data that are not widely published should include copies of the referenced materials. Comments will be posted at *http://www.ntia.doc.gov/internetpolicytaskforce* and *http://csrc.nist.gov.*

1. Quantifying the Economic Impact

Prior to releasing this NOI, the Task Force conducted listening sessions with a wide range of stakeholders in order to understand the issues that have the greatest bearing on cybersecurity preparedness and continued growth of the Internet economy. During those conversations, the Task Force heard that while cybersecurity threats continue to pose challenges for Internet users and services providers, it appears difficult to assess the macro- and microeconomic impact of cybersecurity incidents with current tools. It is hard to manage that which one cannot measure.

Losses related to Internet fraud (*e.g.,* payment fraud, identity theft, credit card fraud) are collected and reported to various government and private entities. However, data that describe the economic impact of cybersecurity incidents more fully and completely, either at the firm or sector level, are not readily available. Not only are losses difficult to quantify with today's tools, but it appears to be difficult to assess in economic terms the return on investments achieved via security measures. Measures of business and consumer investment in security-related activities lack a common reporting entity or information aggregating mechanism.

The availability of authoritative, aggregated data on cybersecurity investments and losses from cyber incidents might yield a quantitative picture of the economic impact of cyber intrusions and attacks. Such data would enable industry and the government to evaluate the severity of cybersecurity threats and emerging trends and to make informed decisions about the trade-offs of different cybersecurity strategies and investment options.

We seek comment on the following questions: How should a data gathering and analysis system (or systems) be fashioned to facilitate the collection of well-defined, consistent metrics to measure the financial impact of cybersecurity incidents and investments in cybersecurity protection? What would be the implementation challenges? Are there adequate incentives for businesses to provide information about security breaches, data security losses, and cybersecurity investments? It would be beneficial from a national perspective to have a greater understanding of the financial costs and benefits of different cybersecurity practices. Does the private sector, however, lack incentives to share information at the firm level? What are reasonable means to acquire the data necessary for greater understanding? At what level of granularity should data be collected and analyzed? What would be the appropriate entity to perform collection and analysis of the data? Aside from assessing the known costs of cyber intrusions and attacks and of cybersecurity measures, what other data would be helpful to better understand the question of whether at the firm, sector and national levels enough is being done to adequately protect the nation's information and communications systems? Can the opportunity costs associated with inadequate security be estimated in some way?

2. Raising Awareness

At the highest level of abstraction, the nation has pursued for the past several years a two-prong strategy for dealing with cybersecurity issues, namely, the continual development of cyber-protection technology and techniques, paired with the sharing of information about those capabilities, about new threats and vulnerabilities, and about data breaches (where required by law). Based on the Task Force's examination to date, these strategies will remain important. The dynamic nature of the cyber risk environment demands continuous innovation in cyber-protection capability. Ongoing improvements in education and other forms of awareness-raising are also necessary, given the fact that a significant proportion of Internet economy participants do not take adequate advantage of readily available cyber-protection tools.

In response to the President's Cyberspace Policy Review, the U.S. Government is stepping up its investment in education and awareness-raising. For example, NIST has assumed overall coordination responsibility for a new National Initiative for

Cybersecurity Education (NICE).[18] NICE has four tracks, each delegated to particular federal agencies. The tracks include: (1) National Cybersecurity Awareness led by the DHS; (2) K–12 and university-level Cybersecurity Education led by the Department of Education and the White House's Office of Science and Technology Policy; (3) the creation of a Federal Cybersecurity Workforce Structure led by the Office of Personnel Management; and (4) the creation of a Cybersecurity Workforce Training effort led by the DOD, DHS, and the Office of the Director of National Intelligence. The Department also recognizes that across the private sector, there are many initiatives—some nationally led, others locally led, some including public-private partnerships—aimed at improving cybersecurity awareness among businesses, consumers, and students.

We seek comment on the efficacy of existing educational efforts, as well as the steps that might be taken to improve them. Are there data that demonstrate that certain educational programs qualify as best practices? What have those who are delivering cybersecurity education learned from their experiences? Which educational plans are succeeding or failing, and have providers of such educational efforts attempted to measure return-on-investment? What additional role, if any, should the government play in cybersecurity education and awareness efforts? What programs, beyond continuing education for IT professionals, workplace training for users, or curriculum development for K–12 or post-secondary institutions, should be developed? Does the private sector require government assistance in developing the kinds of materials and programs that would be useful in this area? Who should be the target audiences?

Given the dynamic nature of cyber threats, it is important for even the most sophisticated commercial entities to be vigilant. One of the best ways to improve defensive capabilities is for good actors to share important information with each other and with appropriate authorities. Yet in our listening sessions, we heard comments that questioned whether enough is being done on this front. Security breach legislation has gone into effect in many states.[19] Nonetheless, our current perception is that for many reasons firms that have experienced cyber intrusions or attacks either do not know with whom to share that information or are reluctant to share.

In the immediate aftermath of a recent, high-profile cyber incident, we heard a variation on this theme. Reportedly, even the most sophisticated small and medium-sized firms are daunted by how complicated it can be to share information on the incidents they have suffered. A successful, targeted intrusion might involve exploitation of a technology vulnerability, loss of customer information, theft of intellectual property or other digital assets, and loss of financial information. Such an exploit might be executed and addressed in a matter of minutes or hours, yet reporting the incident and the losses to the proper officials could consume numerous man-hours, with business owners unsure whether the expenditure of that amount of time yields any benefit to the business.

We seek comment on whether there is adequate awareness of information sharing programs. Are existing information sharing mechanisms adequately-resourced but under-utilized? If so, what deters their use? How can the state of affairs be improved? Are there parts of the business community that do not know the governmental points-of-contact, US–CERT, to report, share information on, and seek guidance regarding cybersecurity incidents? If there are parts of the business community that are unaware of available resources, which parts are they and what steps might help to raise their awareness? Even among that who are aware of the resources and mechanisms available for information sharing and assistance, is there a reluctance to use them? If so, why? Does the government adequately assist businesses in the throes or in the aftermath of a cyber incident? Should the government create a cybersecurity service center to assist the business community in implementing protection measures, sharing information about cyber threats reported by businesses and other sources, and dealing with cybersecurity incidents that occur? What other steps can be taken to improve situational awareness across the business sector?

3. Web Site and Component Security

Increasingly, malware and other malicious content are able to infect computers and other user access devices (*e.g.,* smart phones) in a manner that compromises the integrity of commercial and personal information. Such exploits are often launched through interactive Web sites that end users access online and through the use of external devices (*e.g.,* portable USB drives, digital picture frames). While computer training and consumer education programs can reduce the amount of malware spread through these means by instructing users in safer online practices, there may be other mechanisms or systems that could prove effective in reducing such cyber risks.

In Department of Commerce listening sessions, stakeholders identified improved Web site and component security as another area where modest technology investments might generate large improvements in the level of cybersecurity across the Internet. Should the government alone, the private sector, or the government and private sector collaboratively explore whether third-party verification of Web site and component security is or can prove effective in reducing the proliferation of malware? If so, what measures should be considered? What would be the implementation challenges in deploying such measures?

4. Authentication/Identity (ID) Management

In our listening sessions, several stakeholders urged the Task Force to promote more widespread uptake of state-of-the-art authentication and ID management systems to reduce the incidents of successful cyber intrusions and attacks. Effective authentication and authorization systems establish a user's right to access resources. Many users currently rely on simple password systems for authentication. More sophisticated systems require multiple factors in the authentication process, for example, something the user knows, plus something that the user possesses (*e.g.,* a physical credential or token).[20]

[18] National Initiative for Cybersecurity Education (NICE), *Relationship to President's Education Agenda* (April 19, 2010), *http://www.whitehouse.gov/sites/default/files/rss_viewer/cybersecurity_niceeducation.pdf; see also* Commerce Secretary Gary Locke Announces NIST to Lead National Initiative for Cybersecurity Education, (April 29, 2010), *http://www.commerce.gov/news/press-releases/2010/04/29/commerce-secretary-gary-locke-announces-nist-lead-national-initiative.*

[19] *See, e.g.,* California Database Breach Act, California Civil Code §§ 1798.80–1798.82 (enacted in 2002).

[20] Usability, expense, and support issues are significant considerations in selection of authentication and authorization controls. Most of these systems identify the user. Where the identity of the user is important to a system's access policy, issuance and maintenance of credentials depends on an underlying identity management system. Effective identity management systems establish one party's identity to another party's satisfaction, increasing consumer trust in the use of the Internet, while balancing the security and privacy concerns of all users involved. It is worthwhile to remember that "users" are not a homogeneous group. They consist of individuals, and small, medium, and large enterprises, both public and private. The

The Department seeks comment on the effectiveness of current identity management systems in addressing cybersecurity risks.

On June 25, 2010, the White House released the *National Strategy for Trusted Identities in Cyberspace* for public comment. This strategy promotes a set of options for enhancing on-line security and privacy so that individuals and organizations use trusted, interoperable identity solution as in a manner that promotes confidence, privacy, choice, and innovation to experience efficient and secure access to on line services.[21]

Beyond the measures recommended in the *National Strategy for Trusted Identities in Cyberspace,* what, if any, federal government support is needed to improve authentication/identity management controls, mechanisms, and supporting infrastructures? Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance? If not, what improvements are needed? What specific controls and mechanisms should be implemented? What role should authentication and identity management controls play in a comprehensive set of cybersecurity measures available to commercial organizations? Are the basic infrastructures that underlie the recommended controls and mechanisms already in place? What, if any, new tools or technologies for authentication or identify management are available or are being developed that may address these needs?

How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially? How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures? Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials? If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective? What would be the drawbacks?

How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities? Could a private marketplace for "identity brokers" (*i.e.,* organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively? What would be some of the issues or potential impacts of establishing standards and best practices for private sector identity brokers? Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) Improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems? What are the privacy issues raised by identity management systems and how should those issues be addressed? Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations? What other considerations should factor into government's efforts in this area?

5. Global Engagement

Cybersecurity issues are global. Companies want to design, manufacture, and test their products to make them available for sale in a global marketplace. Many in industry have described fear about the potential for balkanization of the global marketplace due to a proliferation of mandated, sometimes unique cybersecurity standards and conformity assessment requirements among nations—leading to a diverse patchwork of national requirements that can inhibit trade. Such unique national standards and conformity assessment requirements illustrate one way in which some foreign governments seem to be deviating from international norms by using security standards as a de facto entry barrier to protect domestic interests from foreign competition.

We request comment on what other cybersecurity-related problems U.S. businesses may be experiencing when attempting to do business in foreign countries. Please specify discrete areas of concern, such as foreign governments requiring access to product source code. Do U.S. businesses confront unfair competition when competing against nationally controlled companies? If so, in which countries? How can the U.S. Government better encourage the use of internationally accepted cybersecurity standards and practices outside of the United States? Are there more effective ways for the U.S. Government to engage countries that deviate from international norms (*i.e.,* bilaterally, multilaterally, through technical dialogues, at an overarching political level, all of these or through other mechanisms)? Would a set of internationally accepted "cybersecurity principles" in the area of standards and conformity assessment procedures be useful? If so, what role should the Department of Commerce play in promoting such internationally accepted principles?

6. Product Assurance

As noted above, many cybersecurity issues are global, but product assurance is one global issue that warrants particular attention. In the course of conversations with hardware and software developers, the Task Force has heard repeatedly that current domestic and international government product assurance efforts for many products can contribute to costly time-to-market delays, as well as unnecessarily expensive products. Several companies felt that the current U.S. Common Criteria assurance scheme is incompatible with industry product development and maintenance schedules and practices, and that the security assurance derived from many national assurance requirements and evaluation schemes is highly questionable.[22] Additionally, participation in international mutual recognition schemes is, reportedly, so limited that some in industry see themselves as expending very significant resources to satisfy a range of varying security requirements and processes among nations in order to compete in a global market. Industry members have expressed a desire for assistance in improving mutual recognition in the product assurance realm.

We seek comment on the following matters. Do current U.S. Government

diversity of the characteristics among these various categories of users means that each group will make selections among various security solutions based on different criteria that address their unique needs and economic drivers. Privacy considerations also significantly complicate identification based on personally identifiable information. For many purposes, identification needs to simply associate the user's request for access or service with an institutional authorization by the entity that is providing the access or service. By contrast, more sensitive transactions (*e.g.,* online banking or exchange of electronic health records) may require authentication of more of an individual's identifying characteristics. Various audit and enforcement functions benefit from identification of the access with a specific person, but this is not necessary for all use cases.

[21] *National Strategy for Secure Identities in Cyberspace,* at 1 (June 25, 2010), available at *http://www.dhs.gov/xlibrary/assets/ns_tic.pdf.*

[22] More information about the US Common Criteria assurance scheme is available at *http://www.commoncriteriaportal.org/theccra.html.*

product assurance requirements inhibit production of timely security components and/or security-enhanced IT products and systems? Do current assurance processes inhibit innovation? If so, what would be the best way to improve the current U.S. product assurance scheme? What, if any, changes need to be made with respect to international product assurance institutions, standards, and processes (*e.g.,* the Common Criteria Recognition Arrangement)? Should the Common Criteria Recognition Arrangement, the basis for international mutual recognition of cybersecurity product assurance, be expanded to include some of those countries which increasingly stray from international norms? Can useful U.S. Government or international product assurance guidelines be crafted for the current real-world software development environment? To what extent can a security oriented software assurance "tool" be useful in software validation? What elements would be necessary to develop an effective industry-government dialogue to clarify the product assurance goals and challenges, and identify workable solutions?

7. Research and Development

The U.S. Government has a continuing interest in cybersecurity research and development and has funded research on various aspects of security in computing, networking, and data processing for decades. Together with research and development programs at NIST, DOD, and several other agencies, the current unclassified Federal funding in Cyber Security and Information Assurance Research and Development is approximately $350 million per year. One of the goals of the Comprehensive National Cybersecurity Initiative (CNCI) initiated in January 2008 is to develop "leap-ahead" technologies that would achieve orders-of-magnitude improvements in cybersecurity. Based on this directive, in 2009, the agencies of the NITRD Program identified three initial research and development themes to exemplify and motivate future federal cybersecurity game-change research activities.[23] In addition to eliminating redundancies in federally funded cybersecurity research, identifying research gaps, and prioritizing research and development efforts, the Federal government has actively sought to create incentives for private industry and academic institutions to increase their research and development efforts.

The following questions should be considered from the perspective of the Department of Commerce. How can the federal government best promote additional commercial and academic research and development in cybersecurity technology? What particular research and development areas do not receive sufficient attention in the private sector? What cybersecurity disciplines most need research and development resources (*e.g.,* performance metrics, availability, status monitoring, usability, and cost effectiveness)? How effective would a federal government-sponsored "grand challenge program" be at drawing attention to and promoting work on specific technical problems?

8. An Incentives Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

Outside the CIKR sectors, U.S. businesses and consumers generally have resorted to their own devices and evolved their own practices for dealing (or not dealing) with cyber risks. In other words, across large segments of the economy, the level of cybersecurity relies upon the private sector's development, dissemination and adoption of best practices. As Internet usage has grown domestically and abroad, U.S. companies have been faced with a range of Internet-related issues. Based on feedback the Task Force received, the adoption of industry best practices is uneven.

According to some stakeholders, smaller and medium sized businesses may lack the specialized knowledge and resources necessary to meet cybersecurity challenges. Some stakeholders also suggested that the fundamental challenge may be a misalignment of incentives. Still others argued for greater leadership from industry and/or government in developing improved standards for securing cyberspace in a manner that will promote greater economic benefits from an expanding Internet economy. These assertions suggest several questions:

Are existing incentives adequate to address the current risk environment? Do particular business segments lack sufficient incentives to make cybersecurity investments? If so, why? What would be the best way to encourage businesses to make appropriate investments in cybersecurity? Are there public policies or private sector initiatives in the United States or other countries that have successfully increased incentives to make such security investments? Are there disincentives that inhibit cybersecurity investments by firms? If so, what should be done to eliminate them?

Are there examples of cybersecurity best practices that have been (or can be) sufficiently tailored to meet the diverse needs of commercial actors outside the CIKR sectors? Are those best practices well known and understood? Should a set, or sets, of best practices be developed to guide commercial organizations' investment decisions? What role, if any, should the U.S. Government play in their development?

Are minimum performance standards for cybersecurity necessary to protect individual and collective security interests? If so, how should those minimum standards be determined and what could be done to promote their adoption? Would a collaborative government-private sector partnership be appropriate here? What are the merits of providing legal safe-harbors to those individuals and commercial entities that meet a specified minimum security level? By contrast, what would be the merits or implications of enhancing existing frameworks that hold entities accountable for failure to exercise reasonable care and that results in a loss due to inadequate security measures? Should an entity be required to implement a cybersecurity plan or meet a set of minimum security standards prior to receiving government financial guarantees or assistance? Would it be beneficial to utilize government procurement policies to stimulate cybersecurity research, development, and investment generally? How do national security requirements affect the commercial sector's adoption of cybersecurity protection measures?

In addition, companies traditionally carry insurance protection to mitigate various business, natural disaster, and political risks. The growth of the Internet has begun to create a demand for new insurance products that specifically address the risk of Internet connectivity.[24] While there is growth in the adoption of cyber insurance, a compelling economic case for large scale underwriting of cyber risk insurance, apparently, has not been made. As noted above, metrics for establishing the basis for underwriting appear inadequate.

[23] For more information, please visit *http://cybersecurity.nitrd.gov.*

[24] The market for cyber insurance was estimated to be $350 million in 2005, from a negligible amount almost a decade earlier. George Mason University School of Law, Critical Infrastructure Protection Program, *The CIP Report,* at 2 (Sept. 2007), *http://cip.gmu.edu/archive/cip_report_6.3.pdf.*

What role could/should public policy play, if any, in the development of a cyber-risk measurement framework that would be useful in developing insurance products? In the face of growing risk from the increasing volume of cyber threats and vulnerabilities, what data can be made available to companies to support decisions regarding protection through the purchase of insurance products or investing more in cybersecurity protection controls? If companies were able to predictably limit financial risk through specific cyber-insurance coverage at a reliably predictable cost, how would this affect investment in cyber-security programs and infrastructure?

To what extent might insurance providers create incentives or requirements for such investment? In the absence of empirical data to quantify losses from certain types of cyber incidents, what criteria could be used to most accurately and effectively determine premium costs? What, if any, quantitative relationship can be established between investment in security controls and the cost of insurance?

Dated: July 22, 2010.

Gary Locke,

Secretary of Commerce.

Patrick Gallagher,

Director, National Institute of Standards and Technology.

Francisco J. Sánchez,

Under Secretary of Commerce for International Trade, International Trade Administration.

Lawrence E. Strickling,

Assistant Secretary for Communications and Information, National Telecommunications and Information Administration.

[FR Doc. 2010–18507 Filed 7–27–10; 8:45 am]

BILLING CODE 3510–13–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XX57

Fisheries of the Northeast Region; South Atlantic Region

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

ACTION: Notification of determination of overfishing or an overfished condition.

SUMMARY: This action serves as a notice that NMFS, on behalf of the Secretary of Commerce (Secretary), has determined that in the Northeast Region, wolffish is in an overfished condition. In the South Atlantic Region, red grouper is subject to overfishing and is in an overfished condition.

NMFS notifies the appropriate fishery management council (Council) whenever it determines that; overfishing is occurring, a stock is in an overfished condition, or a stock is approaching an overfished condition. If a Council has been notified that a stock is in an overfished condition the Council must, within 2 years, prepare and implement an FMP amendment or proposed regulations to rebuild the affected stock.

FOR FURTHER INFORMATION CONTACT: Mark Nelson, (301) 713–2341.

SUPPLEMENTARY INFORMATION: Pursuant to sections 304(e)(2) and (e)(7) of the Magnuson-Stevens Fishery Conservation and Management Act (Magnuson-Stevens Act), 16 U.S.C. 1854(e)(2) and (e)(7), and implementing regulations at 50 CFR 600.310(e)(2), NMFS, on behalf of the Secretary, notifies Councils whenever it determines; a stock or stock complex is approaching an overfished condition, a stock or stock complex is overfished, or existing action taken to prevent previously identified overfishing or rebuilding a previously identified overfished stock or stock complex has not resulted in adequate progress. NMFS also notifies Councils when it determines a stock or stock complex is subject to overfishing.

For a fishery determined to be overfished or approaching an overfished condition, NMFS also requests that the appropriate Council, or the Secretary, for fisheries under section 302(a)(3) of the Magnuson-Stevens Act, take action to end or prevent overfishing in the fishery and to implement conservation and management measures to rebuild overfished stocks. Councils (or the Secretary) receiving notification that a fishery is overfished must, within 2 years of notification, implement a rebuilding plan, through an FMP Amendment or proposed regulations, which ends overfishing immediately and provides for rebuilding the fishery in accordance with 16 U.S.C. 1854(e)(3)-(4) as implemented by 50 CFR 600.310(j)(2)(ii). Councils receiving a notice that a fishery is approaching an overfished condition must prepare and implement, within two years, an FMP amendment or proposed regulations to prevent overfishing from occurring. When developing rebuilding plans Councils (or the Secretary), in addition to rebuilding the fishery within the shortest time possible in accordance with 16 U.S.C. 1854(e)(4) and 50 CFR 600.310(j)(2)(ii), must ensure that such actions address the requirements to amend the FMP for each affected stock or stock complex to establish a mechanism for specifying and actually specify Annual Catch Limits (ACLs) and Accountability Measures (AMs) to prevent overfishing in accordance with 16 U.S.C. 1853(a)(15) and 50 CFR 600.310(j)(2)(i).

In January 2009, the Northeast Data Poor Stocks Working Group concluded that Atlantic wolffish was in an overfished condition but could not determine whether overfishing was occurring. The New England Fishery Management Council was alerted of this condition on February 6, 2009. However, at that time Atlantic wolffish was not managed under any FMP. Effective with Amendment 16 to the NE Multispecies FMP, in May 2010, wolffish was added as a fishery management unit species. Therefore, this gives public notice that wolffish is has been determined to be in an overfished condition and the overfishing status is unknown.

On July 9, 2010, NMFS informed the South Atlantic Fishery Management Council that based on the 2010 assessment of southern Atlantic coast stock of red grouper, that the stock is currently undergoing overfishing and that the stock is in an overfished condition. Prior to this assessment the previous determination was that overfishing was occurring but the overfished status was unknown.

As noted above, within 2 years of notification of an overfished determination, the respective Council (or the Secretary) must adopt and implement a rebuilding plan, through an FMP Amendment or proposed implementing regulations, which ends overfishing immediately and provides for rebuilding of the stock. In addition, for the fisheries experiencing overfishing, the responsible Councils must propose, and NMFS must adopt, effective ACLs and AMs to end overfishing.

Dated: July 22, 2010.

Emily H. Menashes,

Acting Director, Office of Sustainable Fisheries, National Marine Fisheries Service.

[FR Doc. 2010–18536 Filed 7–27–10; 8:45 am]

BILLING CODE 3510–22–S