include notification and reporting requirements in the unlikely event that any unauthorized access, use, or dissemination of any Census Bureau information would occur.

To reiterate, the information at issue is not a respondent's personal information, rather, it is cyber threat information. E3A does not provide DHS with access to a respondent's personal information. E3A does not currently decrypt respondent information or scan data at rest on Census Bureau information systems.

4. The ADC is concerned that the revised confidentiality pledge ''raises flags on improper use of such information.''

Response: The Act limits DHS's use of information collected pursuant to the Act to the protection of ''information and information systems from cybersecurity risks.'' To be clear, DHS's use of the information for any other purpose would be unlawful.

5. The AAJC suggests that the protections contained in Title 13 and the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), both of which limit the use and disclosure of information collected, should control the information at issue.

Response: Pursuant to the Act, each agency must ''apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system.'' Congress authorized that, notwithstanding the protections previously afforded to information by other laws, such as Title 13, for the purpose of protecting agency information systems from cyber attacks, DHS may access information transiting and traveling to or from an agency information system. Census Bureau employees remain subject to the penalties contained in Title 13, including a federal prison sentence of up to five years and a fine of up to $250,000, or both.

6. The AAJC suggests that either the Census Bureau employees ''perform Einstein 3A functions for Census Bureau internet traffic'' or that ''DHS employees monitoring Census Bureau internet traffic under Einstein 3A take the current Title 13 confidentiality pledge.''

Response: The Act provides DHS access to network traffic transiting or traveling to or from the Census Bureau's information systems, notwithstanding the protections previously afforded to information by other laws, such as Title 13. The Act also requires each agency to ''apply and continue to utilize the capabilities to all information traveling between an agency information system and any information system other than an agency information system.''

In addition to the safeguards contained in the Act, the Census Bureau works with DHS to safeguard respondent information. These additional safeguards cover the collection, retention, use, and disclosure of information. The safeguards also include notification and reporting requirements that would apply in the unlikely event that any unauthorized access, use, or dissemination of any Census Bureau information would occur.

III. Data

Agency: U.S. Census Bureau, Department of Commerce.

Title: Revision of the Confidentiality Pledge under Title 13 United States Code, Section 9.

OMB Control Number: 0607–0993.

Form Number(s): None.

Affected Public: All survey respondents to Census Bureau data collections.

Legal Authority: 44 U.S.C. 3506(e) and 13 U.S.C. Section 9.

This information collection request may be viewed at www.reginfo.gov. Follow the instructions to view Department of Commerce collections currently under review by OMB.

IV. Request for Comments

Comments are invited on the necessity and efficacy of the Census Bureau's revised confidentiality pledge above. Comments submitted in response to this notice will become a matter of public record. Comments should be sent within 30 days of publication of this notice to *OIRA_Submission@omb.eop.gov* or fax to (202)395–5806.

Dated: June 27, 2017.

Sarah Brabson,

NOAA PRA Clearance Officer on behalf of the Department of Commerce.

[FR Doc. 2017–13778 Filed 6–29–17; 8:45 am]

BILLING CODE 3510–07–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

RIN 0648–XF304

Fisheries of the South Atlantic; Southeast Data, Assessment, and Review (SEDAR); Public Meetings; Cancellation

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

ACTION: Notice of change of schedule for SEDAR 56 South Atlantic Black Sea Bass Assessment Webinars.

SUMMARY: The SEDAR 56 assessment of the South Atlantic stock of black seabass will consist of a series webinars. Due to changes to the schedule for the stock assessment, webinars scheduled for Thursday, July 20, 2017 and Wednesday, August 16, 2017 have been cancelled. See **SUPPLEMENTARY INFORMATION.**

DATES: This notice serves to cancel the previously scheduled July 20, 2017 and August 16, 2017 webinars.

ADDRESSES: *SEDAR address:* South Atlantic Fishery Management Council, 4055 Faber Place Drive, Suite 201, N. Charleston, SC 29405; *www.sedarweb.org.*

FOR FURTHER INFORMATION CONTACT: Julia Byrd, SEDAR Coordinator, 4055 Faber Place Drive, Suite 201, North Charleston, SC 29405; phone: (843) 571–4366; email: *julia.byrd@safmc.net.*

SUPPLEMENTARY INFORMATION: The original notice published in the **Federal Register** on March 29, 2017 (82 FR 15495).

The Gulf of Mexico, South Atlantic, and Caribbean Fishery Management Councils, in conjunction with NOAA Fisheries and the Atlantic and Gulf States Marine Fisheries Commissions, have implemented the Southeast Data, Assessment and Review (SEDAR) process, a multi-step method for determining the status of fish stocks in the Southeast Region. The product of the SEDAR webinar series will be a report which compiles and evaluates potential datasets and recommends which datasets are appropriate for assessment analyses, and describes the fisheries, evaluates the status of the stock, estimates biological benchmarks, projects future population conditions, and recommends research and monitoring needs. Participants for SEDAR Workshops are appointed by the Gulf of Mexico, South Atlantic, and Caribbean Fishery Management Councils and NOAA Fisheries Southeast Regional Office, Highly Migratory Species Management Division, and Southeast Fisheries Science Center. Participants include: Data collectors and database managers; stock assessment scientists, biologists, and researchers; constituency representatives including fishermen, environmentalists, and non-governmental organizations (NGOs); international experts; and staff of Councils, Commissions, and state and federal agencies.

During its June 2017 meeting, the South Atlantic Fishery Management

Council made a decision to change the terminal year for the data used on the stock assessment for the South Atlantic black sea bass stock. The decision affects the schedule for the stock assessment and consequently, the scheduled webinars as previously published in the **Federal Register**. An updated schedule will be published once the details are available.

Dated: June 26, 2017.

Jeffrey N. Lonergan,

Acting Deputy Director, Office of Sustainable Fisheries, National marine Fisheries Service.

[FR Doc. 2017–13662 Filed 6–29–17; 8:45 am]

BILLING CODE 3510–22–P

DEPARTMENT OF COMMERCE

National Telecommunications and Information Administration

Multistakeholder Process on Internet of Things Security Upgradability and Patching

AGENCY: National Telecommunications and Information Administration, U.S. Department of Commerce.

ACTION: Notice of open meeting.

SUMMARY: The National Telecommunications and Information Administration (NTIA) will convene a virtual meeting of a multistakeholder process on Internet of Things Security Upgradability and Patching on July 18, 2017. This is the fourth in a series of meetings. For information on prior meetings, see Web site address below.

DATES: The virtual meeting will be held on July 18, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time. See **SUPPLEMENTARY INFORMATION** for details.

ADDRESSES: This is a virtual meeting. NTIA will post links to online content and dial-in information on the multistakeholder process Web site at *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

FOR FURTHER INFORMATION CONTACT: Allan Friedman, National Telecommunications and Information Administration, U.S. Department of Commerce, 1401 Constitution Avenue NW., Room 4725, Washington, DC 20230; telephone: (202) 482–4281; email: *afriedman@ntia.doc.gov.* Please direct media inquiries to NTIA's Office of Public Affairs: (202) 482–7002; email: *press@ntia.doc.gov.*

SUPPLEMENTARY INFORMATION:

Background: In March of 2015 the National Telecommunications and Information Administration issued a Request for Comment to ''identify substantive cybersecurity issues that affect the digital ecosystem and digital economic growth where broad consensus, coordinated action, and the development of best practices could substantially improve security for organizations and consumers.'' [1] We received comments from a range of stakeholders, including trade associations, large companies, cybersecurity startups, civil society organizations and independent computer security experts.[2] The comments recommended a diverse set of issues that might be addressed through the multistakeholder process, including cybersecurity policy and practice in the emerging area of Internet of Things (IoT).

In a separate but related matter in April 2016, NTIA, the Department's Internet Policy Task Force, and its Digital Economy Leadership Team sought comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things.'' [3] Over 130 stakeholders responded with comments addressing many substantive issues and opportunities related to IoT.[4] Security was one of the most common topics raised. Many commenters emphasized the need for a secure lifecycle approach to IoT devices that considers the development, maintenance, and end-of-life phases and decisions for a device.

After reviewing these comments, NTIA announced that the next multistakeholder process on cybersecurity would be on IoT security upgradability and patching.[5] The first meeting of a multistakeholder process on this topic was held on October 19, 2016.[6] A second, virtual meeting of this process was held on January 31, 2017,[7] and a third meeting was held on April 26, 2017.[8]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[9] Unaddressed technical flaws in systems leave the users of software and systems at risk. The nature of these risks varies, and mitigating these risks requires various efforts from the developers and owners of these systems. One of the more common means of mitigation is for the developer or other maintaining party to issue a security patch to address the vulnerability. Patching has become more commonly accepted, even for consumers, as more operating systems and applications shift to visible reminders and automated updates. Yet as one security expert notes, this evolution of the software industry has yet to become the dominant model in IoT.[10]

To help realize the full innovative potential of IoT, users need reasonable assurance that connected devices, embedded systems, and their applications will be secure. A key part of that security is the mitigation of potential security vulnerabilities in IoT devices or applications through patching and security upgrades.

The ultimate objective of the multistakeholder process is to foster a market offering more devices and systems that support security upgrades through increased consumer awareness and understanding. Enabling a thriving market for patchable IoT requires common definitions so that manufacturers and solution providers

[1] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Stakeholder Engagement on Cybersecurity in the Digital Ecosystem, 80 FR 14360, Docket No. 150312253–5253–01 (Mar. 19, 2015), *available at: https://www.ntia.doc.gov/files/ntia/publications/cybersecurity_rfc_03192015.pdf.*

[2] NTIA has posted the public comments received at *https://www.ntia.doc.gov/federal-register-notice/2015/comments-stakeholder-engagement-cybersecurity-digital-ecosystem.*

[3] U.S. Department of Commerce, Internet Policy Task Force, Request for Public Comment, Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things, 81 FR 19956, Docket No 160331306–6306–01 (April 5, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/rfc-potential-roles-government-fostering-advancement-internet-of-things.*

[4] NTIA has posted the public comments received at *https://www.ntia.doc.gov/federal-register-notice/2016/comments-potential-roles-government-fostering-advancement-internet-of-things.*

[5] NTIA, *Increasing the Potential of IoT through Security and Transparency* (Aug. 2, 2016), *available at: https://www.ntia.doc.gov/blog/2016/increasing-potential-iot-through-security-and-transparency.*

[6] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (Sept. 15, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/10192016-meeting-notice-msp-iot-security-upgradability-patching.*

[7] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (April 11, 2017), *available at https://www.ntia.doc.gov/federal-register-notice/2017/notice-04262017-meeting-multistakeholder-process-internet-things.*

[8] NTIA, Notice of Multistakeholder Process on Internet of Things Security Upgradability and Patching Open Meeting (Sept. 15, 2016), *available at: https://www.ntia.doc.gov/federal-register-notice/2016/10192016-meeting-notice-msp-iot-security-upgradability-patching.*

[9] *See, e.g.,* Murugiah Souppaya and Karen Scarfone, *Guide to Enterprise Patch Management Technologies, Special Publication 800–40 Revision 3,* National Institute of Standards and Technology, NIST SP 800–40 (2013) *available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf.*

[10] Bruce Schneier, *The Internet of Things Is Wildly Insecure—And Often Unpatchable,* Wired (Jan. 6, 2014), *available at: https://www.schneier.com/blog/archives/2014/01/security_risks_9.html.*