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). On August 2, 2016, NTIA announced that it would convene a new multistakeholder process on security upgradability and patching for consumer IoT.[3] NTIA subsequently announced that the first meeting of this process would be held on October 19, 2016.[4]

The matter of patching vulnerable systems is now an accepted part of cybersecurity.[5] 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.[6]

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 have shared visions for security, and consumers know what they are purchasing. Currently, no such common, widely accepted definitions exist, so many manufacturers struggle to effectively communicate to consumers the security features of their devices. This is detrimental to the digital ecosystem as a whole, as it does not reward companies that invest in patching, and it prevents consumers from making informed purchasing choices.

At the October 19, 2016, meeting, stakeholders discussed the challenge of patching, and how to scope the discussion. Participants identified five distinct work streams that could help foster better security across the ecosystem, and established working groups to more fully evaluate options in each of these areas.[7] The main objective of the January 31, 2016, meeting is to share progress from the working groups examining the five work streams, and hear feedback from the broader stakeholder community. Stakeholders will also discuss overall progress on the initiative, and identify any additional work that may be needed.

More information about stakeholders' work will be available at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

Time and Date: NTIA will convene a virtual meeting of the multistakeholder process on IoT Security Upgradability and Patching on January 31, 2017, from 2:00 p.m. to 4:30 p.m., Eastern Time. Please refer to NTIA's Web site, *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security,* for the most current information.

Place: 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.*

Other Information: The meeting is open to the public and the press. There will be an opportunity for stakeholders viewing the webcast to participate remotely in the meetings through a moderated conference bridge, including polling functionality. Access details for the meetings are subject to change. Requests for a transcript of the meeting or other auxiliary aids should be directed to Allan Friedman at (202) 482–4281 or *afriedman@ntia.doc.gov* at least seven (7) business days prior to each meeting. Please refer to NTIA's Web site, *http://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security,* for the most current information.

Dated: January 11, 2017.

Kathy D. Smith,

Chief, National Telecommunications and Information Administration.

[FR Doc. 2017–00817 Filed 1–13–17; 8:45 am]

BILLING CODE 3510–60–P

[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] 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.*

[4] 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.*

[5] *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.*

[6] 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.*

[7] *See* NTIA, Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching, at: *https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security.*

DEPARTMENT OF DEFENSE

Office of the Secretary

Charter Amendment of Department of Defense Federal Advisory Committees

AGENCY: Department of Defense.

ACTION: Amendment of Federal Advisory Committee.

SUMMARY: The Department of Defense (DoD) is publishing this notice to announce that it is amending the charter for the Advisory Committee on Arlington National Cemetery.

FOR FURTHER INFORMATION CONTACT: Jim Freeman, Advisory Committee Management Officer for the Department of Defense, 703–692–5952.

SUPPLEMENTARY INFORMATION: This committee's charter is being amended in accordance with the Federal Advisory Committee Act (FACA) of 1972 (5 U.S.C., Appendix, as amended) and 41 CFR 102–3.50(d). The amended charter and contact information for the Committee's Designated Federal Officer (DFO) can be obtained at *http://www.facadatabase.gov/.*

The DoD is amending the charter for the Advisory Committee on Arlington

National Cemetery (''the Committee'') previously published in the **Federal Register** on July 26, 2016 (81 FR 48763). The Committee's charter is being amended to update the number of permanent subcommittees to two and establish the function of the new Remember and Explore subcommittee. All other aspects of the Committee's charter, as previously published, will apply to the Committee.

Dated: January 11, 2017.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2017–00862 Filed 1–13–17; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

Termination of Department of Defense Federal Advisory Committees

AGENCY: Department of Defense.

ACTION: Termination of Federal Advisory Committee.

SUMMARY: The Department of Defense (DoD) is publishing this notice to announce that it is terminating the Advisory Council on Dependents' Education.

FOR FURTHER INFORMATION CONTACT: Jim Freeman, Advisory Committee Management Officer for the Department of Defense, 703–692–5952.

SUPPLEMENTARY INFORMATION: Section 576 of the National Defense Authorization Act for Fiscal Year 2017 (Pub. L. 114–328) rescinds 22 U.S.C. 929, which is the statutory authority for the Advisory Council on Dependents' Education (''the Council''). Therefore, the Department of Defense is terminating the Council.

Dated: January 11, 2017.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2017–00868 Filed 1–13–17; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Office of the Secretary

[Docket ID DOD–2008–HA–0180]

Submission for OMB Review; Comment Request

ACTION: Notice.

SUMMARY: The Department of Defense has submitted to OMB for clearance, the following proposal for collection of information under the provisions of the Paperwork Reduction Act.

DATES: Consideration will be given to all comments received by February 16, 2017.

FOR FURTHER INFORMATION CONTACT: Fred Licari, 571–372–0493.

SUPPLEMENTARY INFORMATION:

Title, Associated Form and OMB Number: Professional Qualifications Medical/Peer Reviewers; CHAMPUS Form 780; OMB Control Number 0720–0005.

Type of Request: Reinstatement.

Number of Respondents: 60.

Responses per Respondent: 1.

Annual Responses: 60.

Average Burden per Response: 20 minutes.

Annual Burden Hours: 20.

Needs and Uses: The information collection requirement is necessary to obtain and record the professional qualifications of medical and peer reviewers utilized within TRICARE®. The form is included as an exhibit in an appeal or hearing case file as evidence of the reviewer's professional qualifications to review the medical documentation contained in the case file.

Affected Public: Business or other for profit.

Frequency: On occasion.

Respondent's Obligation: Voluntary.

OMB Desk Officer: Ms. Stephanie Tatham.

Comments and recommendations on the proposed information collection should be emailed to Ms. Stephanie Tatham, DoD Desk Officer, at *Oira_submission@omb.eop.gov.* Please identify the proposed information collection by DoD Desk Officer and the Docket ID number and title of the information collection.

You may also submit comments and recommendations, identified by Docket ID number and title, by the following method:

• *Federal eRulemaking Portal: http://www.regulations.gov.* Follow the instructions for submitting comments.

Instructions: All submissions received must include the agency name, Docket ID number and title for this **Federal Register** document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at *http://www.regulations.gov* as they are received without change, including any personal identifiers or contact information.

DOD Clearance Officer: Mr. Frederick Licari.

Written requests for copies of the information collection proposal should be sent to Mr. Licari at WHS/ESD Directives Division, 4800 Mark Center Drive, East Tower, Suite 03F09, Alexandria, VA 22350–3100.

Dated: January 11, 2017.

Aaron Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2017–00829 Filed 1–13–17; 8:45 am]

BILLING CODE 5001–06–P

DEPARTMENT OF DEFENSE

Department of the Navy

Meeting of the Ocean Research Advisory Panel

AGENCY: Department of the Navy, DOD.

ACTION: Notice of open meeting.

SUMMARY: The Ocean Research Advisory Panel (ORAP) will hold a regularly scheduled meeting. The meeting will be open to the public.

DATES: The meeting will be held on Wednesday, January 11, 2017 from 9:00 a.m. to 11:00 a.m., Eastern Time. Members of the public should submit their comments in advance of the meeting to the meeting Point of Contact. Due to circumstances beyond the control of the Designated Federal Officer and the Department of Defense, the Ocean Research Advisory Panel was unable to provide public notification of its meeting of January 11, 2017, as required by 41 CFR 102–3.150(a). Accordingly, the Advisory Committee Management Officer for the Department of Defense, pursuant to 41 CFR 102–3.150(b), waives the 15-calendar day notification requirement.

ADDRESSES: This will be a teleconference. For access, connect to: *https://global.gotomeeting.com/join/822051381.* The call-in number will be: (312) 757–3121, with access code: 822–051–381.

FOR FURTHER INFORMATION CONTACT: CDR Joel W. Feldmeier, Office of Naval Research, 875 North Randolph Street Suite 1425, Arlington, VA 22203–1995, telephone 703–696–5121.

SUPPLEMENTARY INFORMATION: This notice of open meeting is provided in accordance with the Federal Advisory Committee Act (5 U.S.C. App. 2). The meeting will include discussions on ocean research, resource management, and other current issues in the ocean science and management communities.