

of this meeting is to update the Committee on the progress of the NCST investigation of Hurricane Maria's effects on the U.S. territory of Puerto Rico. The goals of the investigation will be to characterize: (1) The wind environment and technical conditions associated with deaths and injuries; (2) the performance of representative critical buildings, and designated safe areas in those buildings, including their dependence on lifelines; and (3) the performance of emergency communications systems and the public's response to such communications. The agenda may change to accommodate Committee business. The final agenda will be posted on the NIST website at <https://www.nist.gov/topics/disaster-failure-studies/national-construction-safety-team-ncst/advisory-committee>.

**DATES:** The NCST Advisory Committee will meet on Wednesday, May 16, 2018 from 1:00 p.m. to 4:00 p.m. Eastern Time.

**ADDRESSES:** The meeting will be held via webinar. For instructions on how to participate in the meeting, please see the **SUPPLEMENTARY INFORMATION** section of this notice.

**FOR FURTHER INFORMATION CONTACT:** Benjamin Davis, Management and Program Analyst, Community Resilience Program, Engineering Laboratory, NIST, 100 Bureau Drive, Mail Stop 8615, Gaithersburg, Maryland 20899-8604. Mr. Davis' email address is [Benjamin.Davis@nist.gov](mailto:Benjamin.Davis@nist.gov); and his phone number is (301) 975-6071.

**SUPPLEMENTARY INFORMATION:** The Committee was established pursuant to Section 11 of the NCST Act (Pub. L. 107-231, codified at 15 U.S.C. 7301 *et seq.*). The Committee is currently composed of six members, appointed by the Director of NIST, who were selected on the basis of established records of distinguished service in their professional community and their knowledge of issues affecting the National Construction Safety Teams. The Committee advises the Director of NIST on carrying out the NCST Act; reviews the procedures developed for conducting investigations; and reviews the reports issued documenting investigations. Background information on the NCST Act and information on the NCST Advisory Committee is available at <https://www.nist.gov/topics/disaster-failure-studies/national-construction-safety-team-ncst/advisory-committee>.

Pursuant to the Federal Advisory Committee Act, as amended, 5 U.S.C. App., notice is hereby given that the NCST Advisory Committee will meet on Wednesday, May 16, 2018 from 1:00

p.m. to 4:00 p.m. Eastern Time. The meeting will be open to the public. The meeting will be held via webinar. The primary purpose of this meeting is to update the Committee on the progress of the NCST investigation of Hurricane Maria's effects on the U.S. territory of Puerto Rico. The goals of the investigation will be to characterize: (1) The wind environment and technical conditions associated with deaths and injuries; (2) the performance of representative critical buildings, and designated safe areas in those buildings, including their dependence on lifelines; and (3) the performance of emergency communications systems and the public's response to such communications. The agenda may change to accommodate Committee business. The final agenda will be posted on the NIST website at <https://www.nist.gov/topics/disaster-failure-studies/national-construction-safety-team-ncst/advisory-committee-meetings>.

Individuals and representatives of organizations who would like to offer comments and suggestions related to items on the Committee's agenda for this meeting are invited to request a place on the agenda. Approximately 15 minutes will be reserved near the conclusion of the meeting for public comments, and speaking times will be assigned on a first-come, first-served basis. The amount of time per speaker will be determined by the number of requests received, but is likely to be three minutes each. Questions from the public will not be considered during this period. All those wishing to speak must submit their request by email to the attention of Mr. Benjamin Davis, [Benjamin.Davis@nist.gov](mailto:Benjamin.Davis@nist.gov), by 5:00 p.m. Eastern Time, Friday, May 11, 2018. Speakers who wish to expand upon their oral statements, those who had wished to speak but could not be accommodated on the agenda, and those who were unable to attend are invited to submit written statements to the NCST, National Institute of Standards and Technology, 100 Bureau Drive, MS 8604, Gaithersburg, Maryland 20899-8604, or electronically by email to [Benjamin.Davis@nist.gov](mailto:Benjamin.Davis@nist.gov).

To participate in the meeting, please submit your first and last name, email address, and phone number to Benjamin Davis at [Benjamin.Davis@nist.gov](mailto:Benjamin.Davis@nist.gov) or (301) 975-6071. After pre-registering, participants will be provided with detailed instructions on how to join the meeting remotely. Anyone wishing to attend this meeting must register by 5:00 p.m. Eastern Time, Friday, May 11, 2018, to attend. Please submit your full name, email address, and phone number to Benjamin Davis at [\[nist.gov\]\(mailto:nist.gov\); his phone number is \(301\) 975-6071.](mailto:Benjamin.Davis@</a></p></div><div data-bbox=)

**Kevin A. Kimball,**  
*Chief of Staff.*

[FR Doc. 2018-10163 Filed 5-11-18; 8:45 am]

**BILLING CODE 3510-13-P**

## DEPARTMENT OF COMMERCE

### National Institute of Standards and Technology

#### Announcing Request for Comments on Lightweight Cryptography Requirements and Evaluation Criteria

**AGENCY:** National Institute of Standards and Technology (NIST), Commerce.

**ACTION:** Notice; request for comments.

**SUMMARY:** The National Institute of Standards and Technology (NIST) is requesting comments on a proposed process to solicit, evaluate, and standardize one or more lightweight cryptographic algorithms. Current NIST cryptographic standards were designed to perform well on general-purpose computing platforms, and may not be suitable for some constrained computing environments. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center website: <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

**DATES:** Comments must be received on or before June 28, 2018.

**ADDRESSES:** Comments may be sent electronically to [lightweight-crypto@nist.gov](mailto:lightweight-crypto@nist.gov) with "Comment on Lightweight Cryptography Requirements and Evaluation Criteria" in the subject line. Written comments may also be submitted by mail to Information Technology Laboratory, ATTN: Lightweight Cryptography Comments, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930.

Comments received in response to this notice will be published electronically at <https://csrc.nist.gov/Projects/Lightweight-Cryptography>, so commenters should not include information they do not wish to be posted (e.g., personal or confidential business information).

**FOR FURTHER INFORMATION CONTACT:** Dr. Kerry McKay, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8930, Gaithersburg, MD 20899-8930, email: [kerry.mckay@nist.gov](mailto:kerry.mckay@nist.gov), by telephone (301) 975-4969. Technical inquiries regarding the proposed draft acceptability

requirements, submission requirements, or the evaluation criteria should be sent electronically to *lightweight-crypto@nist.gov*.

A public email list has been set up for announcements, as well as a forum to discuss the standardization effort being initiated by NIST. For directions on how to subscribe, please visit <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

**SUPPLEMENTARY INFORMATION:** The deployment of small computing devices such as RFID tags, industrial controllers, sensor nodes and smart cards is becoming much more common. The shift from desktop computers to small devices brings a wide range of new security and privacy concerns. It is challenging to apply conventional cryptographic standards to small devices, because the tradeoff between security, performance and resource requirements was optimized for desktop and server environments, and this makes the standards difficult or impossible to implement in resource-constrained devices. Therefore, when current NIST-approved algorithms can be engineered to fit within the limited resources of constrained environments, their performance may not be acceptable.

There are several emerging areas in which highly-constrained devices are interconnected, working in concert to accomplish some task. Examples of these areas include: Automotive systems, sensor networks, healthcare, distributed control systems, the Internet of Things (IoT), cyber-physical systems, and the smart grid. In recent years, there has been increased demand for cryptographic standards that are tailored for constrained devices. NIST has decided to create a portfolio of lightweight cryptographic algorithms, designed for limited use in applications and environments where cryptographic operations are performed by constrained devices that are unable to use existing NIST standards.

Lightweight cryptography is a subfield of cryptography that aims to provide solutions tailored for resource-constrained devices. There has been a significant amount of work done by the academic community related to lightweight cryptography; this work includes efficient implementations of conventional cryptography standards, and the design and analysis of new lightweight primitives and protocols. The purpose of this notice is to solicit comments on the draft minimum acceptability requirements, submission requirements, evaluation criteria, and evaluation process of candidate

algorithms from the public, the cryptographic community, academic and research communities, manufacturers, voluntary standards organizations, and federal, state, and local government organizations so that their needs can be considered in the process of developing new lightweight cryptography standards. The draft requirements and evaluation criteria are available on the NIST Computer Security Resource Center website: <https://csrc.nist.gov/Projects/Lightweight-Cryptography>.

**Authority:** In accordance with the Information Technology Management Reform Act of 1996 (Pub. L. 104-106) and the Federal Information Security Management Act of 2002 (Pub. L. 107-347), the Secretary of Commerce is authorized to approve Federal Information Processing Standards. NIST activities to develop computer security standards to protect federal sensitive (unclassified) information systems are undertaken pursuant to specific responsibilities assigned to NIST by Section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3), as amended.

**Kevin A. Kimball,**  
*Chief of Staff.*

[FR Doc. 2018-10127 Filed 5-11-18; 8:45 am]

**BILLING CODE 3510-13-P**

## DEPARTMENT OF COMMERCE

### National Oceanic and Atmospheric Administration

**RIN 0648-XG238**

#### Gulf of Mexico Fishery Management Council; Public Meeting

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

**ACTION:** Notice of a public meeting.

**SUMMARY:** The Gulf of Mexico Fishery Management Council will hold a two day meeting of its Standing and Reef Fish Scientific and Statistical Committees (SSC).

**DATES:** The meeting will convene on Thursday, May 31, 2018, 8:30 a.m. to 5:30 p.m., and Friday, June 1, 2018, 8:30 a.m. to 2:30 p.m. EDT.

**ADDRESSES:** The meeting will be held in the Gulf Council's Conference Room.

*Council address:* Gulf of Mexico Fishery Management Council, 2203 N Lois Avenue, Suite 1100, Tampa, FL 33607; telephone: (813) 348-1630.

**FOR FURTHER INFORMATION CONTACT:** Steven Atran, Senior Fishery Biologist, Gulf of Mexico Fishery Management

Council; [steven.atran@gulfcouncil.org](mailto:steven.atran@gulfcouncil.org), telephone: (813) 348-1630.

#### SUPPLEMENTARY INFORMATION:

**Day 1—Thursday, May 31, 2018; 8:30 a.m.—5:30 p.m.**

- I. Introductions and Adoption of Agenda
- II. Approval of March 26–27, 2018 SSC Minutes
- III. Selection of SSC representative at June 18–22, 2018 Council meeting in Key West, FL

#### *Standing and Reef Fish SSC Session*

- IV. SEDAR 37 Update (FWC hogfish assessment)
  - a. Review of assessment
  - b. OFL and ABC recommendations
- V. SEDAR 51 (gray snapper benchmark assessment)
  - a. Review of assessment
  - b. OFL and ABC recommendations
- VI. SEDAR 52 (red snapper standard assessment)
  - a. Review of assessment
  - b. Discard mortality estimates of red snapper by sector
  - c. Estimate of the reduction in mortality (numbers of fish) for red snapper from use of venting and descending devices
  - d. OFL and ABC recommendations

**Day 2—Friday, June 1, 2018; 8:30 a.m.—2:30 p.m.**

- VI. Continuation of SEDAR 52 (red snapper standard assessment)
  - VII. SEDAR 64 (yellowtail snapper benchmark assessment)
    - a. Review and approval of terms of reference
    - b. Review and approval of schedule
    - c. Data, assessment, and review workshop appointments
  - VIII. Discussion on Best Scientific Information Available
    - a. Review of National Standard 2
    - b. Council Coordinating Committee comments
  - IX. Draft Reef Fish Amendment 48/Red Drum Amendment 5
    - a. Review of MSY Proxy Paper, “Establishing Stock Status Determination Criteria for Fisheries with High Discards and Uncertain Recruitment” by Goethel et al.
    - b. Review of draft amendment
  - X. Tentative 2018 SSC Meeting Dates
  - XI. Other Business—Adjourn
- The meeting will be broadcast via webinar. You may register for the webinar by visiting [www.gulfcouncil.org](http://www.gulfcouncil.org) and clicking on the SSC meeting on the calendar. <https://attendee.gotowebinar.com/register/3383291116212545537>. The Agenda is subject to change, and the latest version along with other meeting materials will