the data collection plans and instruments, contact: Dr. Dina Paltoo, Director, Scientific Data Sharing Policy Division, Office of Science Policy, NIH, 6705 Rockledge Dr., Suite 750, Bethesda, MD 20892, or call non-toll-free number (301) 496–9838, or Email your request, including your address to: *SciencePolicy@mail.nih.gov.*

**SUPPLEMENTARY INFORMATION:** This proposed information collection was previously published in the **Federal Register** on April 2, 2018, page 14018 (83 FR 14018) and allowed 60 days for public comment. No public comments were received. The purpose of this notice is to allow an additional 30 days for public comment. The Office of the Director (OD), National Institutes of Health, may not conduct or sponsor, and the respondent is not required to respond to, an information collection that has been extended, revised, or implemented on or after October 1, 1995, unless it displays a currently valid OMB control number.

In compliance with Section 3507(a)(1)(D) of the Paperwork Reduction Act of 1995, the National Institutes of Health (NIH) has submitted to the Office of Management and Budget (OMB) a request for review and approval of the information collection listed below.

*Proposed Collection:* The Genetic Testing Registry, 0925–0651, Expiration Date 07/31/2018—EXTENSION, Office of the Director (OD), National Institutes of Health (NIH).

*Need and Use of Information Collection:* Clinical laboratory tests are available for more than 10,000 genetic conditions. The Genetic Testing Registry (GTR) provides a centralized, online location for test developers, manufacturers, and researchers to voluntarily submit detailed information about the availability and scientific basis of their genetic tests. The GTR is of value to clinicians by providing information about the accuracy, validity, and usefulness of genetic tests. The GTR also highlights evidence gaps where additional research is needed.

OMB approval is requested for 3 years. There are no costs to respondents other than their time. The total estimated annualized burden hours are 4,198.

ESTIMATED ANNUALIZED BURDEN HOURS

| Type of respondent | Form name | Number of respondents | Number of responses per respondent | Average time per response (in hours) | Total annual burden hour |
|---|---|---|---|---|---|
| Laboratory Personnel Using Bulk Submission | Minimal Fields | 313 | 25 | 18/60 | 2,348 |
| Optional Fields. | ..... | 313 | 25 | 6/60 | 783 |
| Laboratory Personnel Not Using Bulk Submission | Minimal Fields | 64 | 25 | 30/60 | 800 |
| Optional Fields. | ..... | 64 | 25 | 10/60 | 267 |
| Total | ..... | 377 | 18,850 | ..... | 4,198 |

Dated: June 28, 2018.

**Lawrence A. Tabak,**

*Principal Deputy Director, National Institutes of Health.*

[FR Doc. 2018–14435 Filed 7–3–18; 8:45 am]

**BILLING CODE 4140–01–P**

## DEPARTMENT OF HEALTH AND HUMAN SERVICES

### Substance Abuse and Mental Health Services Administration

### Center for Mental Health Services; Notice of Meeting

Pursuant to Public Law 92–463, notice is hereby given that the Substance Abuse and Mental Health Services Administration (SAMHSA), Center for Mental Health Services (CMHS) National Advisory Council (NAC) will meet on August 1, 2018, from 9:00 a.m. to 5:00 p.m. E.D.T. The NAC will convene in both open and closed sessions on August 1, 2018.

The closed portion of the meeting will include discussion of grant applications that were reviewed by SAMHSA's Initial Review Groups, and involves an examination of confidential financial and business information as well as personal information concerning the applications. Therefore, the meeting will be closed to the public from 9:00 a.m. to 9:30 a.m., as determined by the Assistant Secretary for Mental Health and Substance Use, SAMHSA in accordance with Title 5 U.S.C. § 552b(c)(4) and (6) and Title 5 U.S.C. App. 2, § 10(d).

The remainder of this meeting will be open to the public from 9:30 a.m. to 5:00 p.m., E.D.T., to include discussion of the Center's policy issues, updates on the Interdepartmental Serious Mental Illness Coordinating Committee, presentations on Suicide Prevention, School Mental Health/Child Trauma and a conversation with the Assistant Secretary for Mental Health and Substance Use.

Attendance by the public will be limited to available space. Interested persons may present data, information, or views, orally or in writing, on issues pending before the council. Written submissions should be forwarded to the contact person (below) on or before July 17, 2018. Oral presentations from the public will be scheduled at the conclusion of the meeting on Wednesday, August 1, 2018. Five minutes will be allotted for each presentation. Meeting information and a roster of Council members may be obtained either by accessing the SAMHSA Council website at *http://www.samhsa.gov/about-us/advisory-councils/cmhs-national-advisory-council* or by contacting Ms. Pamela Foote (see contact information below).

The meeting can be accessed via telephone. To obtain the conference call-in number and access code, submit written or brief oral comments, or request special accommodations for persons with disabilities, please register at the SAMHSA's Advisory Council website at *http://nac.samhsa.gov/Registration/meetingsRegistration.aspx,* or contact Pamela Foote (see contact information below).

*Committee Name:* Substance Abuse and Mental Health Services Administration Center for Mental Health Services National Advisory Council.

*Dates/Time/Type:* Wednesday, August 1, 2018, 9:00 a.m. to 9:30 a.m. EDT: CLOSED; Wednesday, August 1, 2018, 9:30 a.m. to 5:00 p.m. EDT: OPEN.

*Place:* SAMHSA, 5600 Fishers Lane, 5th Floor, Conference Room 5W11, Rockville, Maryland 20857.

*Contact:* Pamela Foote, Designated Federal Official, SAMHSA CMHS National Advisory Council, 5600 Fishers Lane, Room 14E53C, Rockville, Maryland 20857, Telephone: (240) 276–1279, Fax: (301) 480–8491, *Email: pamela.foote@samhsa.hhs.gov.*

**Carlos Castillo,**

*Committee Management Officer.*

[FR Doc. 2018–14381 Filed 7–3–18; 8:45 am]

**BILLING CODE 4162–20–P**

## DEPARTMENT OF HOMELAND SECURITY

**[Docket No. DHS–2018–0023]**

### Nationwide Cyber Security Review Assessment

**AGENCY:** Office of Cybersecurity and Communications (CS&C), National Protection and Programs Directorate (NPPD), Department of Homeland Security (DHS).

**ACTION:** 60-Day Notice and request for comments; New Collection, 1670—NEW.

**SUMMARY:** DHS NPPD CS&C will submit the following information collection request (ICR) to the Office of Management and Budget (OMB) for review and clearance in accordance with the Paperwork Reduction Act of 1995.

**DATES:** Comments are encouraged and will be accepted until September 4, 2018.

**ADDRESSES:** You may submit comments, identified by docket number DHS–2018–0023, by one of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Please follow the instructions for submitting comments.
- *Email: SLTTCyber@HQ.DHS.GOV.* Please include docket number DHS–2018–0023 in the subject line of the message.
- *Mail:* Written comments and questions about this Information Collection Request should be forwarded to DHS/NPPD/CS&C, ATTN: 1670–NEW, Donna Beach, 245 Murray Lane, SW, Mail Stop 0612, Arlington, VA 20528.

*Instructions:* All submissions received must include the words ''Department of Homeland Security'' and docket number DHS–2018–0023. Comments received will be posted without alteration at *http://www.regulations.gov,* including any personal information provided.

Comments submitted in response to this notice may be made available to the public through relevant websites. For this reason, please do not include in your comments information of a confidential nature, such as sensitive personal information or proprietary information. If you send an email comment, your email address will be automatically captured and included as part of the comment that is placed in the public docket and made available on the internet. Please note that responses to this public comment request containing any routine notice about the confidentiality of the communication will be treated as public comments that may be made available to the public notwithstanding the inclusion of the routine notice.

**FOR FURTHER INFORMATION CONTACT:** For specific questions related to collection activities, please contact Donna Beach at 703–705–6213 or at *SLTTCyber@HQ.DHS.GOV.*

**SUPPLEMENTARY INFORMATION:** In its reports to the Department of Homeland Security Appropriations Act, 2010, Congress requested a Nationwide Cyber Security Review (NCSR) from the National Cyber Security Division (NCSD), the predecessor organization of the Stakeholder Engagement and Cyber Infrastructure Resilience (SECIR) division. S. Rep. No. 111–31, at 91 (2009), H.R. Rep. No. 111–298, at 96 (2009). The House Conference Report accompanying the Department of Homeland Security Appropriations Act, 2010 ''note[d] the importance of a comprehensive effort to assess the security level of cyberspace at all levels of government'' and directed DHS to ''develop the necessary tools for all levels of government to complete a cyber network security assessment so that a full measure of gaps and capabilities can be completed in the near future.'' H.R. Rep. No. 111–298, at 96 (2009). Concurrently, in its report accompanying the Department of Homeland Security Appropriations Bill, 2010, the Senate Committee on Appropriations recommended that DHS ''report on the status of cyber security measures in place, and gaps in all 50 States and the largest urban areas.'' S. Rep. No. 111–31, at 91 (2009).

The Homeland Security Act of 2002, as amended, established ''a national cybersecurity and communications integration center [NCCIC] . . . to carry out certain responsibilities of the Under Secretary,'' including the provision of assessments. 6 U.S.C. 148(b). The Act also directs the composition of the NCCIC to include an entity that collaborates with State and local governments on cybersecurity risks and incidents, and has entered into a voluntary information sharing relationship with the NCCIC. 6 U.S.C. 148(d)(1)(E). The Multistate Information Sharing and Analysis Center (MS–ISAC) currently fulfills this function. NPPD funds the MS–ISAC through a Cooperative Agreement and maintains a close relationship with this entity. As part of the Cooperative Agreement, DHS directs the MS–ISAC to produce the NCSR as contemplated by Congress.

Generally, NPPD has authority to perform risk and vulnerability assessments for Federal and non-Federal entities, with consent and upon request. The NCCIC performs these assessments in accordance with its authority to provide voluntary technical assistance to Federal and non-Federal entities. See 6 U.S.C. 148(c)(6), 143(2). This authority is consistent with the Department's responsibility to ''[c]onduct comprehensive assessments of the vulnerabilities of the Nation's critical infrastructure in coordination with the SSAs [Sector-Specific Agencies] and in collaboration with SLTT [State, Local, Tribal, and Territorial] entities and critical infrastructure owners and operators.'' Presidential Policy Directive (PPD)–21, at 3. A private sector entity or state and local government agency also has discretion to use a self-assessment tool offered by NPPD or request NPPD to perform an on-site risk and vulnerability assessment. See 6 U.S.C. 148(c)(6), 143(2), 6 U.S.C. 121(d)(2). The NCSR is a voluntary annual self-assessment.

Upon submission of the first NCSR report in March 2012, Congress further clarified its expectation ''that this survey will be updated every other year so that progress may be charted and further areas of concern may be identified.'' S. Rep. No. 112–169, at 100 (2012). In each subsequent year, Congress has referenced this NCSR in its explanatory comments and recommendations accompanying the Department of Homeland Security Appropriations. Consistent with Congressional mandates, SECIR developed the NCSR to measure the gaps and capabilities of cybersecurity programs within SLTT governments. Using the anonymous results of the NCSR, DHS delivers a bi-annual summary report to Congress that provides a broad picture of the current cybersecurity gaps & capabilities of SLTT governments across the nation.

The assessment allows SLTT governments to manage cybersecurity related risks through the NIST Cybersecurity Framework (CSF) which consists of best practices, standards and guidelines. In efforts of continuously providing Congress with an accurate representation of the SLTT