discussions and does not provide guidance or reflect FDA’s current thinking on this subject. The workshop report was posted on FDA’s website on July 11, 2018.

II. Electronic Access


Dated: August 17, 2018.

Leslie Kux,
Associate Commissioner for Policy.

[FR Doc. 2018–18132 Filed 8–22–18; 8:45 am]
BILLING CODE 4164–01–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Advisory Council on the National Health Service Corps

AGENCY: Health Resources and Service Administration (HRSA), Department of Health and Human Services (HHS).

ACTION: Notice of meeting.

SUMMARY: The National Advisory Council on the National Health Service Corps (NACNHSC) has scheduled a public meeting. Information about NACNHSC and the agenda for this meeting can be found on the NACNHSC website at https://nhsc.hrsa.gov/about/national-advisory-council-nhsc/index.html.

DATES: September 17, 2018, 9:00 a.m.–2:30 p.m., E.T.

ADDRESSES: This meeting will be held in person and will offer virtual access through teleconference and webinar. The address for the meeting is 5600 Fishers Lane, Room 5W37, Rockville, Maryland 20857.

• Conference call-in number: 1–800–238–9007; passcode: 155333.
• Webinar link is https://hrsconnectsolutions.com/nacnhsc.

FOR FURTHER INFORMATION CONTACT: Diane Fabiyi-King, Designated Federal Official (DFO), Division of National Health Service Corps, HRSA, 5600 Fishers Lane, Room 14N110, Rockville, Maryland 20857; 301–443–3609; or DFabiyi-King@hrsa.gov.

SUPPLEMENTARY INFORMATION: NACNHSC consults, advises, and makes recommendations to the HHS Secretary and the HRSA Administrator with respect to their responsibilities. NACNHSC also reviews and comments on regulations promulgated by the Secretary under Subpart II, Part D of Title III of the Public Health Service Act.

During the September 2018 meetings, NACNHSC will continue its discussion from the May 15, 2018, meeting to develop recommendations on the current NHSC focus areas and finalize policy recommendations to the Secretary and the HRSA Administrator. The current circumstances to strengthen the healthcare workforce and NHSC’s role in the expansion and improvement of access to quality opioid and substance use disorder treatment in rural and underserved areas is an important opportunity for NACNHSC to add its voice. For this reason, NACNHSC will develop comprehensive policy recommendations and a framework to articulate a clear vision and mission statement that aligns with the BHW and HRSA strategic plan. An agenda will be posted on the NACNHSC website prior to the meeting. Agenda items are subject to change as priorities dictate.

Members of the public will have the opportunity to provide comments. Oral comments will be honored in the order they are requested and may be limited as time allows. Requests to make oral comments or provide written comments to the NACNHSC should be sent to Monica-Tia Bullock by email at MBullock@hrsa.gov at least 3 business days prior to the meeting. Council members are given copies of all written statements submitted from the public. Any further public participation will be solely at the discretion of the Chair, with approval of the DFO. Registration through the designated contact for the public comment session is required. Individuals who plan to attend and need special assistance or another reasonable accommodation should notify Monica-Tia Bullock using the email address listed above at least 10 business days prior to the meeting. Since this meeting occurs in a federal government building, attendees must go through a security check to enter the building. Non-U.S. Citizen attendees must notify HRSA of their planned attendance at least 10 business days prior to the meeting in order to facilitate their entry into the building. All attendees are required to present government-issued identification prior to entry.

Amy P. McNulty,
Acting Director, Division of the Executive Secretary.

[FR Doc. 2018–18143 Filed 8–22–18; 8:45 am]
BILLING CODE 4165–15–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

Privacy Act of 1974; System of Records

AGENCY: Office of Security and Strategic Information (OSSI), Immediate Office of the Secretary (IOS), Department of Health and Human Services (HHS).

ACTION: Notice of a new system of records.

SUMMARY: In accordance with the requirements of the Privacy Act of 1974, as amended (the Act), the Department of Health and Human Services (HHS) is providing notice of the establishment of a new system of records, System No. 09–09–1701, HHS Insider Threat Program Records. The new system of records will cover records about individuals, retrieved by personal identifier, which are compiled and used by the Department’s Office of Security and Strategic Information (OSSI), within the Immediate Office of the Secretary (IOS), to administer the Department’s insider threat program. Because the records in this system of records include investigatory material compiled for law enforcement purposes and information classified in the interest of national security, elsewhere in today’s Federal Register HHS has published a Notice of Proposed Rulemaking (NPRM) to exempt this system of records from certain requirements of the Privacy Act, pursuant to subsections (k)(1) and (k)(2) of the Act. The system of records is more fully described in the SUPPLEMENTARY INFORMATION section of this notice and in the System of Records Notice (SORN) published in this notice.

DATES: This system of records is applicable August 23, 2018 with the exception of the routine uses and exemptions. Written comments on the SORN should be submitted by September 24, 2018. If HHS receives no significant adverse comment within the specified comment period, the routine uses will be applicable on September 24, 2018. If any timely significant adverse comment is received, HHS will publish a revised system of records. The exemptions will be applicable following publication of a Final Rule.

ADDRESSES: The public should address written comments on the proposed system of records to insiderthreat@hhs.gov or to the HHS Office of Security and Strategic Information (OSSI), 200 Independence Avenue SW, Washington, DC 20201.

FOR FURTHER INFORMATION CONTACT: General questions about the system of records may be submitted to Michael Schmoyer, Ph.D., Assistant Deputy...
The Insider Threat Program system of records includes investigatory material compiled for law enforcement purposes and information classified in the interest of national security. While OSSI does not perform criminal law enforcement activity as its principal function, OSSI may compile in System No. 09–90–1701 material obtained from other agencies or components which perform as their principal function activities pertaining to the enforcement of criminal laws, and which have exempted their records from certain Privacy Act requirements, based on 5 U.S.C. 552a(j)(2). All other investigatory material compiled for law enforcement purposes is eligible to be exempted from certain Privacy Act requirements based on 5 U.S.C. 552a(k)(2). Information classified in the interest of national security is eligible to be exempted from certain Privacy Act requirements, based on 5 U.S.C. 552a(k)(1). The Department’s NPRM published in today’s Federal Register proposes to establish these exemptions for System No. 09–90–1701.

- Law enforcement investigatory material compiled in this system of records that is from another system of records in which such material was exempted from access and other requirements of the Privacy Act (the Act) based on 5 U.S.C. 552a(j)(2) will be exempt in this system of records on the same basis (5 U.S.C. 552a(j)(2)) and from the same requirements as in the source system. The requirements from which records described in 5 U.S.C. 552a(j)(2) are eligible to be exempted are: (c)(3)–(4); (d)(1)–(4); (e)(1)–(3), (e)(4)(G)–(I), (e)(5), (e)(8), (e)(12); (f); (g); and (h).
- All other law enforcement investigatory material in System No. 09–90–1701 will be exempt, based on 5 U.S.C. 552a(k)(2), from the requirements in subsections (c)(3), (d)(1)–(4), (e)(1), (e)(4)(G)–(I), and (f) of the Act. However, if any individual is denied a right, privilege, or benefit to which the individual would otherwise be entitled by Federal law or for which the individual would otherwise be eligible, access will be granted, except to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality.
- Information in this system of records that is classified in the interest of national security will be exempt, based on 5 U.S.C. 552a(k)(1), from the requirements in subsections (c)(3), (d)(1)–(4), (e)(1), (e)(4)(G)–(I), and (f) of the Act.

Note that this system of records does not cover investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualification for federal civilian employment, military service, federal contracts, or access to classified information. Such material is covered by other HHS systems of records (i.e., 09–90–0002 with respect to HHS Office of Inspector General determinations, and 09–90–0020 as to all other HHS determinations) which have been exempted from access and other Privacy Act requirements based on 5 U.S.C. 552a(k)(5).

SYSTEM NAME AND NUMBER:
HHS Insider Threat Program Records, 09–90–1701

SECURITY CLASSIFICATION:
Classified and unclassified.

SYSTEM LOCATION:
HHS Office of Security and Strategic Information (OSSI), 200 Independence Avenue SW, Washington, DC 20201.

SYSTEM MANAGER(S):
Assistant Deputy Secretary for National Security, HHS Office of Security and Strategic Information (OSSI), 200 Independence Avenue SW, Washington, DC 20201.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:


**Purpose(s) of the System:**

The purpose of the system is to support a program of insider threat detection and prevention that is consistent with guidance and standards developed by the National Insider Threat Task Force, ensures the responsible sharing and safeguarding of information, and provides appropriate privacy and civil liberties protections. Records will be used on a need-to-know basis to manage insider threat matters; facilitate inside threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries and investigations; identify threats to Department resources, including threats to the Department’s personnel, facilities, and information assets (including, in particular, classified networks and information); track tips and referrals of potential insider threats to internal and external partners; provide information for statistical reports; and meet other insider threat program requirements.

**Categories of Individuals Covered by the System:**

The categories of individuals covered by this system are HHS insiders, defined as any person with authorized access to any HHS resource to include personnel, facilities, information, equipment, networks or systems. Such persons include present and former HHS employees, members of joint task forces under the purview of HHS, contractors, detailees, assignees, interns, visitors, and guests.

For the purposes of this system of records, sensitive information includes information classified pursuant to Executive Orders 13526, 12829, and 13549 and unclassified information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and U.S. Government-wide policies falling under the program established by Executive Order 13556.

**Categories of Records in the System:**

The system will include the categories of records:

A. Records derived from lawful HHS security investigations, including authorized physical, personnel, and communications security investigations, and information systems security analysis and reporting, such as:

- Responses to information requested by official questionnaires (e.g., SF 86 Questionnaire for National Security Positions) that include: Full name, former names and aliases; date and place of birth; social security number; height and weight; hair and eye color; gender; ethnicity and race; biometric data; mother’s maiden name; personal identity verification (PIV) number; current and former home and work addresses, phone numbers, and email addresses; employment history; military record information; selective service registration record; residential history; education history and degrees earned; names of associates and references with their contact information; citizenship information; passport information; driver’s license information; identifying numbers from access control passes or identification cards; criminal history; civil court actions; prior personnel security eligibility, investigative, and adjudicative information, including information collected through continuous evaluation; mental health history; records related to drug or alcohol use; financial record information; credit reports; the name, date and place of birth, social security number, and citizenship information for spouse or cohabitant; the name and marriage information for current and former spouse(s); the citizenship, name, date and place of birth, and address for relatives;

- Reports furnished to HHS or collected by HHS in connection with personnel security investigations, continuous evaluation for eligibility for access to classified information, and insider threat detection programs operated by HHS pursuant to Federal laws and Executive Orders and HHS policies, including information derived from: Responses to information requested on foreign contacts and activities; association records; information on loyalty to the United States;

- Records relating to the management and operation of HHS personnel and physical security, including information derived from: Personnel security adjudications and financial disclosure filings; nondisclosure agreements; document control registries; courier authorization requests; derivative classification unique identifiers; requests for access to sensitive compartmented information (SCI); security violation files; travel records; foreign contact reports; briefing and debriefing statements for special programs, positions designated as sensitive; polygraph examination results; logs of computer activities on all HHS information technology (IT) systems or any IT systems accessed by HHS personnel with security clearances; facility access records; and

- Reports of investigation regarding security violations, including:

  - Individual statements or affidavits and correspondence; incident reports; drug test results; investigative records of a criminal, civil, or administrative nature; letters, emails, memoranda and reports; exhibits, evidence, statements, and affidavits; inquiries relating to suspected security violations; and recommended remedial actions for possible security violations.

B. Summaries or reports about potential insider threats, from:
• Reports of investigation regarding security violations, including:
  Statements, declarations, affidavits and correspondence; incident reports;
  investigative records of a criminal, civil or administrative nature; letters, emails,
  memoranda, and reports; exhibits and evidence; and, recommended remedial
  or corrective actions for security violations; reports about potential
  insider threats regarding: Personnel user names and aliases, levels of network
  access, audit data, information regarding misuse of HHS devices, information
  regarding unauthorized use of
  removable media, and logs of printer,
  copier, and facsimile machine use;
  • Information collected through user activity monitoring, which is the
  technical capability to observe and
  record the actions and activities of all
  users, at any time, on a computer
  network monitored by HHS, even if not
  controlled by HHS, thereof in order to
deter, detect, and mitigate insider
  threats as well as to support authorized
  investigations. Such information may
  include key strokes, screen captures,
  and content transmitted via email, chat,
  or data import or export;
  • Reports about potential insider
  threats from records of usage of
government telephone systems,
including the telephone number
initiating the call, the telephone number
receiving the call, and the date and time
of the call;
• Payroll information, travel
  vouchers, benefits information, credit
  reports, equal employment opportunity
  complaints, performance evaluations,
disciplinary files, training records,
substance abuse and mental health
records of individuals undergoing law
enforcement action or presenting an
identifiable imminent threat, counseling
statements, outside work and activities
requests, and personal contact records;
and
  • Particularly sensitive or protected
  information, including information held
  by special access programs, law
  enforcement, inspector general, or other
  investigative sources or programs.
Access to such information may require
additional approval by the senior HHS
official who is responsible for managing
and overseeing the program.

C. Information related to investigative
or analytical efforts by HHS insider
threat program personnel, including:
• Identifying threats to HHS
personnel, property, facilities, and
information; information obtained from
Intelligence Community members, the
Federal Bureau of Investigation, or from
other agencies or organizations about
individuals known or suspected of
being engaged in conduct constituting,

preparing for, aiding, or relating to an
insider threat, including espionage or
unauthorized disclosure of classified
national security information;
• Publicly available information,
such as information regarding: Arrests
and detentions; real property;
bankruptcy; liens or holds on property;
vehicles; licensure (including
professional and pilot’s licenses,
firearms and explosive permits);
business licenses and filings; and from
social media;
• Information provided by record
subjects and individual members of the
public; and
• Information provided by
individuals who report known or
suspected insider threats.

D. Reports about potential insider
threats obtained through the
management and operation of the HHS
Operating or Staff Division insider
threat programs, including:
• Documentation pertaining to
investigative or analytical efforts by
HHS insider threat program personnel
to identify threats to HHS personnel,
property, facilities, and information;
• Records collated to examine
information technology events and other
information that could reveal potential
insider threat activities; and
• Travel records.

E. Reports about potential insider
threats obtained from other Federal
Government sources, including:
• Documentation obtained from
Intelligence Community members, the
Federal Bureau of Investigation, or from
other agencies or organizations
pertaining to individuals known or
suspected of being engaged in conduct
constituting, preparing for, aiding, or
relating to an insider threat, including
espionage or unauthorized disclosure of
classified national security information; and
• Intelligence reports and database
query results relating to individuals
covered by this system.

RECORD SOURCE CATEGORIES:
Information in the system will be
received from Department officials,
employees, contractors, and other
individuals who are associated with or
represent HHS; officials from other
foreign, federal, tribal, state, and local
government agencies and organizations;
non-government, commercial, public,
and private agencies and organizations;
complainants, informants, suspects, and
witnesses; and from relevant records,
including counterintelligence and
security databases and files; personnel
security databases and files; HHS
human resources databases and files;
Office of the Chief Information
Officer
and information assurance databases
and files; information collected through
user activity monitoring; HHS telephone
usage records; federal, state, tribal,
territorial, and local law enforcement
and investigatory records; Inspector
General records; available U.S.
Government intelligence and
counterintelligence reporting
information and analytic products
pertaining to adversarial threats; other
Federal agencies; and publicly available
information.

ROUTINE USES OF RECORDS MAINTAINED IN THE
SYSTEM, INCLUDING CATEGORIES OF USERS AND
PURPOSES OF SUCH USES:
HHS may disclose records about an
individual from this system of records
to parties outside HHS, without the
individual’s prior written consent,
pursuant to these routine uses:
1. Records may disclosed to agency
contractors, consultants, or others who
have been engaged by the agency to
assist with accomplishment of an HHS
function relating to the purposes of this
system of records and who need to have
access to the records in order to assist
HHS.
2. Records may be disclosed to any
person, organization, or governmental
entity in order to notify them of a
serious terrorist threat for the purpose of
guarding against or responding to the
threat.
3. Records may be disclosed to third
parties during the course of an
investigation to the extent necessary to
obtain information pertinent to the
investigation
4. Records may be disclosed to a
federal, state, or local agency, or other
appropriate entities or individuals, or
through established liaison channels to
selected foreign governments, in order
to enable the intelligence agency with
the relevant authority and responsibility
for the matter to carry out its
responsibilities under the National
Security Act of 1947 as amended, the
CIA act of 1949 as amended, Executive
Order 12333 or any successor order,
applicable national security directives,
or classified implementing procedures
approved by the Attorney General and
promulgated pursuant to such statutes,
orders or directives.
5. Factual information the disclosure
of which would be in the public interest
and which would not constitute an
unwarranted invasion of personal
privacy may be disclosed to the news
media or the general public.
6. Where a record, either alone or in
conjunction with other information,
indicates a violation or potential
violation of law, whether civil, criminal,
or regulatory in nature, and whether
arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the agency concerned, whether federal, state, local, tribal, territorial, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, or the rule, regulation, or order issued pursuant thereto.

7. Records may be disclosed to an appropriate federal, state, local, tribal, territorial, foreign, or international agency, if the information is relevant and necessary to a requesting agency’s decision concerning the hiring or retention of an individual, or issuance of a security clearance, license, contract, grant, delegation or designation of authority, or other benefit, or if the information is relevant and necessary to a HHS decision concerning the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, delegation or designation of authority, or other benefit and disclosure is appropriate to the proper performance of the official duties of the person making the request.

8. Records may be disclosed to the Department of Justice (DOJ) or to a court or other tribunal when:
   a. HHS or any of its components; or
   b. any employee of HHS acting in the employee’s official capacity; or
   c. any employee of HHS acting in the employee’s individual capacity where the DOJ or HHS has agreed to represent the employee; or
   d. the United States Government, is a party to a proceeding or has an interest in such proceeding and the disclosure of such records is deemed by the agency to be relevant and necessary to the proceeding.

9. Records may be disclosed to a congressional office from the record of an individual in response to a written inquiry from the congressional office made at the written request of that individual.

10. Records may be disclosed to representatives of the National Archives and Records Administration during records management inspections conducted pursuant to 44 U.S.C. 2904 and 2906.

11. Records may be disclosed to appropriate agencies, entities, and persons when (1) HHS suspects or has confirmed that there has been a breach of the system of records, (2) HHS has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, HHS (including its information systems, programs, and operations), the federal government, or national security, and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with HHS’s efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

12. Records may be disclosed to another federal agency or federal entity, when HHS determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the federal government, or national security, resulting from a suspected or confirmed breach.

13. Records may be disclosed to the U.S. Department of Homeland Security (DHS) if captured in an intrusion detection system used by HHS and DHS pursuant to a DHS cybersecurity program that monitors internet traffic to and from federal government computer networks to prevent a variety of types of cybersecurity incidents.

   The disclosures authorized by publication of the above routine uses pursuant to 5 U.S.C. 552a(b)(3) are in addition to the following disclosures which HHS may make based on other authorizations:
   - Disclosures authorized by the subject individual’s prior written consent pursuant to 5 U.S.C. 552a(b).
     For example, another agency conducting a background investigation or assessment may request information from this system of records using the consent form that the subject individual signed.
   - Disclosures authorized directly in the Privacy Act at 5 U.S.C. 552a(b)(1), (2) and (b)(4)–(11). For example, another agency conducting a law enforcement activity may request information from this system of records by making the request in accordance with 5 U.S.C. 552a(b)(7).

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

   Records will be stored in hard copy files and electronic media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

   Records will be retrieved by an individual record subject’s name, SSN, or PIV identification number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

   The records in this system of records are covered by National Archives and Records Administration General Records Schedule 5.6, items 230 and 240. Records determined to be associated with an insider threat or to have potential to be associated with an insider threat are destroyed 25 years after the date the threat was discovered, but a longer retention is authorized if required for business use. User attributable data collected to monitor user activities on a network to enable insider threat programs and activities to identify and evaluate anomalous activity, identify and assess misuse or exploitation, or support authorized inquiries and investigations, is destroyed five years after an inquiry was opened, but a longer retention is authorized if required for business use.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

   Safeguards will conform to the HHS Information Security and Privacy Program, http://www.hhs.gov/ocio/securityprivacy/index.html. Information will be safeguarded in accordance with applicable laws, rules and policies, including the HHS Information Technology Security Program Handbook, all pertinent National Institutes of Standards and Technology (NIST) publications, and OMB Circular A–130, Managing Information as a Strategic Resource. Records will be protected from unauthorized access through appropriate administrative, physical, and technical safeguards. These safeguards include protecting the facilities where records are stored or accessed with security guards, badges and cameras; securing hard-copy records in locked file cabinets, file rooms or offices during off-duty hours; controlling access to physical locations where records are maintained and used by means of combination locks and identification badges issued only to authorized users; limiting access to electronic databases to authorized users based on roles and two-factor authentication (user ID and password), using a secured operating system protected by encryption, firewalls, and intrusion detection systems, requiring encryption for records stored on removable media, and training personnel in Privacy Act and information security requirements. Records that are eligible for destruction will be disposed of using secure destruction methods prescribed by NIST SP 800–88.
An individual seeking access to records about him or her in this system of records should submit an access request to the System Manager identified in the “System Manager” section of this SORN, and must follow the access procedures contained in the HHS Privacy Act regulations, 45 CFR part 5b (currently located in section 5b.5). The individual’s right of access under the Privacy Act will be subject to the exemptions promulgated for this system of records. Records compiled in reasonable anticipation of a civil action or proceeding are excluded from the Privacy Act access requirement in all systems of records as provided in 5 U.S.C. 552a(d)(5).

NOTIFICATION PROCEDURES:
An individual who wishes to know if this system contains records about him or her should submit a notification request to the System Manager identified in the “System Manager” section of this SORN, and must follow the notification procedures contained in the HHS Privacy Act regulations, 45 CFR part 5b (currently located in section 5b.7). The individual’s right of notification will be subject to the exemptions promulgated for this system of records.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:
Upon completion of the Department’s pending rulemaking (i.e., when a Final Rule has been published in the Federal Register and has become effective based on the Notice of Proposed Rulemaking published elsewhere in today’s Federal Register), this system of records will be exempt from access and other requirements of the Privacy Act, as follows:

- Material compiled in this system of records that is from another system of records in which such material was exempted from access and other requirements of the Privacy Act (the Act) based on 5 U.S.C. 552a(j)(2) will be exempt from this system of records on the same basis (5 U.S.C. 552a(j)(2)) and from the same requirements as in the source system. The requirements from which records described in 5 U.S.C. 552a(j)(2) are eligible to be exempted are: (c)(3)–(4); (d)(1)–(4); (e)(1)–(3), (e)(4)(G)–(I), (e)(5), (e)(8), (e)(12); (f); (g); and (h).
- All other law enforcement investigatory material in System No. 09–90–1701 will be exempt, based on 5 U.S.C. 552a(k)(2), from the requirements in subsections (c)(3), (d)(1)–(4), (e)(1), (e)(4)(G)–(I), and (f) of the Act. However, if any individual is denied a right, privilege, or benefit to which the individual would otherwise be entitled by Federal law or for which the individual would otherwise be eligible, access will be granted, except to the extent that the disclosure would reveal the identity of a source who furnished information to the Government under an express promise of confidentiality.
- Information in this system of records that is classified in the interest of national security will be exempt, based on 5 U.S.C. 552a(k)(1), from the requirements in subsections (c)(3), (d)(1)–(4), (e)(1), (e)(4)(G)–(I), and (f) of the Act.

HISTORY:
None.

Dated: June 29, 2018.

Michael Schmoyer,
Assistant Deputy Secretary for National Security.

BILLING CODE 4151–17–P

DEPARTMENT OF HEALTH AND HUMAN SERVICES

National Institutes of Health

National Institute on Aging; Notice of Closed Meeting

Pursuant to section 10(d) of the Federal Advisory Committee Act, as amended, notice is hereby given of the following meeting.

The meeting will be closed to the public in accordance with the provisions set forth in sections 552b(c)(4) and 552b(c)(6), Title 5 U.S.C., as amended. The grant applications and the discussions could disclose confidential trade secrets or commercial property such as patentable material, and personal information concerning individuals associated with the grant applications, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy.

Name of Committee: Center for Scientific Review Special Emphasis Panel; PAR Panel

Agenda: To review and evaluate grant applications.

Place: National Institute on Aging, Gateway Building, Suite 2W200, 7201 Wisconsin Avenue, Bethesda, MD 20892.

Contact Person: Melanie J. Pantoja, Program Analyst, Office of Federal Advisory Committee Policy.

BILLING CODE 4140–01–P