www.copyright.gov/policy/music-streaming-fraud. If electronic submission of comments is not feasible due to lack of access to a computer or the internet, please contact the Office using the contact information below for special instructions.

FOR FURTHER INFORMATION CONTACT: Rhea Efthimiadis, Assistant to the General Counsel, by email at *USCOGeneralCounsel@copyright.gov* or by telephone at (202) 707–8350.

SUPPLEMENTARY INFORMATION: On October 7, 2026, the U.S. Copyright Office issued a notice of inquiry seeking comments from the public on several questions regarding music streaming fraud.[1] The notice set a deadline for initial written comments to be submitted by November 23, 2026, and for reply comments to be submitted by December 21, 2026.

To ensure that members of the public have sufficient time to prepare responses to the Office's questions, and to ensure that the Office can proceed on a timely basis with its inquiry into the issues identified in its notice with the benefit of a complete record, the Office is extending the comment submission deadlines as set forth here. Initial written comments will now be due no later than 5:00 p.m. Eastern Time on December 18, 2026. Reply comments will be due no later than 11:59 p.m. Eastern Time on January 29, 2027.

Dated: November 3, 2026.

Emily L. Chapuis,

General Counsel and Associate Register of Copyrights.

[FR Doc. 2026–22602 Filed 11–4–26; 8:45 am]

BILLING CODE 1410–30–P

[1] 91 FR 64188 (Oct. 7, 2026).

NATIONAL SCIENCE FOUNDATION

Privacy Act of 1974; System of Records

AGENCY: National Science Foundation.

ACTION: Notice of a new system of records.

SUMMARY: NSF proposes to establish Privacy Act systems of records to track and manage matters pertaining to the agency's awardee compliance program, reasonable accommodation program, and sexual assault and harassment prevention and response program. These systems support the agency's efforts to ensure that complaints and inquiries received or handled by these programs are timely and appropriately acknowledged, processed, and documented.

DATES: Persons wishing to comment on these proposed agency systems may do so on or before December 7, 2026. These new systems of records will become final and effective without further notice on December 7, 2026 unless modified by subsequent notice to reflect public comments, if any, on the proposed system(s).

ADDRESSES: You may submit comments on these proposed systems, identified by ''NSF–84,'' ''NSF–85,'' and/or ''NSF–86,'' as applicable, by any of the following methods:

- *Federal eRulemaking Portal: http://www.regulations.gov.* Docket number NSF–2026–OTR–0067. Follow the instructions for submitting comments.
- *Email:* Tom Boger, Acting Senior Agency Official for Privacy (SAOP), *privacy@nsf.gov.* Include ''NSF–84,'' ''NSF–85,'' and/or ''NSF–86,'' as applicable, in the subject line of the message.
- *Mail:* Tom Boger, Acting SAOP, Office of the Chief Information Officer, NSF, 401 Dulany Street, Alexandria, VA 22314.

NSF intends to post all in-scope comments publicly. All comments submitted in response to this Notice will become a matter of public record. Do not include any information of a sensitive or confidential nature about yourself or others.

FOR FURTHER INFORMATION CONTACT: For information regarding the proposed Privacy Act systems of records, contact Tom Boger, Acting SAOP, Office of the Chief Information Officer, NSF, 401 Dulany Street, Alexandria, VA 22314, *privacy@nsf.gov.* For information regarding NSF's awardee compliance contact NSF Office of Civil Rights, 401 Dulany Street, Alexandria, VA 22314 *ACB@nsf.gov,* and for information on the reasonable accommodation program, contact the NSF Office of Civil Rights, 401 Dulany Street, Alexandria, VA 22314, *rarequests@nsf.gov.* For information regarding NSF's sexual assault and harassment prevention and response program, contact Renée Ferranti, Program Manager, NSF, 401 Dulany Street, Alexandria, VA, *saferscience@nsf.gov.*

SUPPLEMENTARY INFORMATION: In accordance with the Privacy Act of 1974, 5 U.S.C. 552a, NSF is publishing a proposed Privacy Act system of records notice (SORN) for the case management system in support of each of the NSF administrative programs described below.

NSF–84: Awardee Compliance Case Management System

This SORN is intended to establish the NSF Office of Civil Rights (OCR) electronic case management system (CMS) for receiving, tracking, managing, and responding to complaints or reports received from victims, witnesses, or other individuals alleging discrimination, harassment, or retaliation in programs and activities that receive financial assistance from NSF (*e.g.,* NSF grants, cooperative agreements). Individuals may file a complaint or report through the online Web-based CMS by registering and creating a CMS user account. (Witnesses or other third parties may also file a complaint or report of discrimination, harassment, or retaliation on behalf of another individual through the CMS, but only with that individual's consent.) For Privacy Act purposes, all complaints, reports, or other records in the CMS are to be treated as records ''about'' the subject individual (*i.e.,* victim of the alleged discrimination, harassment, or retaliation), *see* 5 U.S.C. 552a(a)(4) (defining Privacy Act ''record'') and are to be maintained and retrieved only by the case number or other identifier personally assigned to the subject individual, and not by any other third-party individual who may also be identified in such records (*e.g.,* alleged violator, witnesses).

To the extent the system's online form constitutes an information collection activity subject to U.S. Office of Management & Budget (OMB) approval under the Paperwork Reduction Act (PRA), the form was approved by OMB and assigned Control No. 3145–0288 (National Science Foundation Office of Civil Rights Case Management System) on April 8, 2026.

NSF–85: Reasonable Accommodation Request E-Filing System

This SORN is intended to establish the NSF OCR electronic filing system pertaining to NSF employees, job applicants, and individuals conducting business at NSF who have requested a ''reasonable accommodation'' under applicable Federal law (*e.g.,* assistive technology, accessibility, support services, or other adjustments or modifications to the work environment under the Rehabilitation Act of 1973, as amended). Individuals may initiate such a request electronically by registering and creating an account in the online Web-based e-filing system, which will then allow them to submit information about their accommodation request, and to view the status of any request that they originally created in the system.

Account registration data, reasonable accommodation requests, and other system records collected by the program to process or track the status of such requests are to be maintained and retrieved by the name, email, or other personally assigned identifier of the subject individual for whom the reasonable accommodation is being requested.

Information about reasonable accommodations may also be found in health and safety records for NSF staff and visitors (NSF–78) and administrative records compiled on users of NSF's health unit or other NSF workplace health programs (NSF–79). *See* 86 FR 66340 (Nov. 22, 2021). Those record systems are separately managed by NSF's human resources division, and OCR is not proposing to duplicate those records in maintaining its own system to track, manage, or respond to reasonable accommodation requests filed with OCR.

NSF–86: Sexual Assault and Harassment Prevention and Response Program (SAHPR) Case Management Tracking System

This SORN is intended to establish an electronic CMS in support of NSF's SAHPR program, which serves as a central agency point of contact for coordinating the agency's response to sexual assault, sexual harassment, and stalking incidents occurring in connection with NSF-funded programs or activities, and for overseeing training and other comprehensive practices to prevent such incidents. The SAHPR program does not provide legal advice or conduct investigations but supports individuals impacted by sexual assault, sexual harassment and stalking, by providing information on how and where to report incidents and available advocacy and supportive resources, helping them with accessing support during investigative and medical processes, safety planning, and assisting them with obtaining other related support or service needs. Accordingly, the SAHPR system records may include notes or information about the reported incident and how it was handled or addressed. These notes or information may include, for example, whether the matter was referred to: NSF OCR, if it involves a complaint or report of harassment, discrimination, or retaliation handled and reviewed by that office, *see* SORN NSF–84, discussed above; to the NSF's Office of Inspector General (OIG), which maintains its own investigatory records system, *see* NSF–52, 83 FR 8903 (Mar. 1, 2018); to the individual's institution for investigation; or to law enforcement, human resources, or other appropriate authorities. The SAHPR CMS records are to be maintained by a case number assigned to the incident or inquiry and retrieved from the system by that number or the name of the impacted individual. Incident records may in some cases include information about third parties (*e.g.,* alleged offenders, witnesses) but system records are not maintained or retrieved by those individuals' names or any other personally assigned identifiers. Such third-party information is collected and maintained in the impacted individual's records only as needed to assist the SAHPR program in tracking and coordinating the agency's response to the incident.

The agency's SAHPR system is separate from OIG's investigatory records system and also separate from other systems of service records that may be maintained by private organizations with whom NSF has contracted or otherwise arranged to provide individuals with confidential helpline support, personal counseling, and advocacy, or other informational or support services. For the protection of privacy and to ensure that individuals can access and utilize those services on a confidential and/or anonymous basis, the third-party service records are not part of NSF agency records, are not intended to be accessed or maintained by or on behalf of NSF, and are not to be disclosed or shared by these service providers unless required or authorized by law (*e.g.,* mandatory reporting to child or adult protective services, or where the individual has consented to disclosure).

None of the proposed Privacy Act systems of records discussed above is intended to duplicate or overlap with any other existing NSF or Government-wide systems of records under the Privacy Act. In accordance with subsection (r) the Privacy Act, at 5 U.S.C. 552a(r), and Office of Management and Budget (OMB) Circular No. A–108, NSF, in addition to publication of this notice in the **Federal Register**, is also submitting notice of the establishment of these system of records to OMB and to the appropriate Congressional committees. All NSF SORNs, including these SORNs, once made final, may be viewed at *www.nsf.gov/* privacy.

NSF–84

SYSTEM NAME AND NUMBER:

Awardee Compliance Case Management System, NSF–84.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

U.S. National Science Foundation (NSF), 401 Dulany Street, Alexandria, VA 22314. Records may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage.

SYSTEM MANAGER(S):

Office Head, Office of Civil Rights (OCR), NSF.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Title VI of the Civil Rights Act of 1964, 42 U.S.C. 2000d *et seq.* (race, color, national origin discrimination in Federally assisted programs and activities); Title IX of the Educational Amendments of 1972, 20 U.S.C. 1681 *et seq.* (sex discrimination); Section 504 of the Rehabilitation Act of 1973, 29 U.S.C. 794 (disability discrimination); Age Discrimination Act of 1975, 42 U.S.C. 6101 *et seq.;* Executive Order 13160 (Nondiscrimination in Federally Conducted Education & Training Programs); 45 CFR parts 605, 606, 611, 617, and 618 (NSF implementing regulations); 2 CFR 200.300 (statutory and national policy requirements for Federal awards); and other authorities, as applicable.

PURPOSE(S) OF THE SYSTEM:

To receive, evaluate, process, investigate, and resolve complaints or reports of alleged discrimination, harassment, or retaliation by recipients of NSF awards or funds, including awardee institutions, principal investigators (PIs), co-PIs or others in programs or activities receiving NSF financial assistance. Records are used to determine whether there is jurisdiction under applicable civil rights statutes and NSF implementing regulations for NSF to investigate the complaint and, if appropriate, require remedial or other action, or whether to refer the matter to the agency's Office of Inspector General (OIG), the relevant institution(s), and/or other agencies or entities for investigation, mediation, or other appropriate action, if any. Records may also be used in connection with conducting compliance reviews or other relevant assessments, analyses, and audits; to produce reports; and otherwise used to evaluate or ensure compliance by NSF recipients with codes of conduct, notification, or other requirements under award terms and conditions and applicable Federal antidiscrimination, equal employment, disability, and related laws, regulations, orders, and policies.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

Individuals who file complaints alleging discrimination, harassment, or retaliation by awardee institutions, PIs, co-PIs, or others in programs or activities receiving Federal financial assistance from NSF. Records in this system are considered records about the complainant (subject individual) and maintained and retrieved by that individual's name or other personally assigned identifier (*e.g.,* case or tracking number), including records of complaints or reports that a third-party individual may file on behalf of and with the consent of the subject individual.

CATEGORIES OF RECORDS IN THE SYSTEM:

Name, email address, phone number, and other contact information of the complainant (subject individual) and, where applicable, of third-party individuals authorized to file a complaint or report in the system on the subject individual's behalf, including the filing individual's account-related data (*e.g.,* password, system-generated account activity log); description of the alleged discrimination, harassment, or retaliation; the identity of individual(s) allegedly engaged in or responsible for such conduct; the awardee (recipient) institution(s); information about witnesses, if any; proposed or requested action or remedies; whether the complaint has been filed in any other forum; additional supporting documentation, if any; and consent/release form(s) for NSF to investigate and/or disclose the subject individual's records to awardee institution(s) or others. If NSF determines that it has jurisdiction and the complaint is accepted for investigation, additional information relevant to the case may be collected, compiled, generated, and maintained as part of the complaint record and case file.

RECORD SOURCE CATEGORIES:

Complainants (subject individuals), other individuals (*e.g.,* legal representative, family member) whom the subject individual has authorized to file the complaint or report on the subject individual's behalf; witnesses, other agencies or awardee institutions, affected parties and/or respondents (investigatory targets), NSF employees, contractors, publicly available information (*e.g.,* online databases, sites, news media), and other third-party sources.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The following NSF standard routine uses apply:

1. Members of Congress. Information from a system may be disclosed to congressional offices in response to inquiries from the congressional offices made at the request of the individual to whom the record pertains.

2. Freedom of Information Act/Privacy Act Compliance. Information from a system may be disclosed to the Department of Justice or the Office of Management and Budget to obtain advice regarding NSF's obligations under the Freedom of Information Act and the Privacy Act.

3. Counsel. Information from a system may be disclosed to NSF's legal representatives, including the Department of Justice and other outside counsel, where the agency is a party in litigation or has an interest in litigation and the information is relevant and necessary to such litigation, including when any of the following is a party to the litigation or has an interest in such litigation: (a) NSF, or any component thereof; (b) any NSF employee in his or her official capacity; (c) any NSF employee in his or her individual capacity, where the Department of Justice has agreed to, or is considering a request to, represent the employee; or (d) the United States, where NSF determines that litigation is likely to affect the agency or any of its components.

4. National Archives and Records Administration (NARA). Information from a system may be disclosed to representatives of the National Archives and Records Administration (NARA) during records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

5. Response to an Actual or Suspected Compromise or Breach of Personally Identifiable Information. NSF may disclose information from the system:

a. to appropriate agencies, entities, and persons when (1) NSF suspects or has confirmed that there has been a breach of the system of records; (2) NSF has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NSF (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 NSF efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

b. to another Federal agency or Federal entity, when NSF 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.

6. Courts. Information from a system may be disclosed to the Department of Justice or other agencies in the event of a pending court or formal administrative proceeding, when the information is relevant and necessary to that proceeding, for the purpose of representing the government, or in the course of presenting evidence, or the information may be produced to parties or counsel involved in the proceeding in the course of pre-trial discovery.

7. Contractors. Information from a system may be disclosed to contractors, agents, experts, consultants, or others performing work on a contract, service, cooperative agreement, job, or other activity for NSF and who have a need to access the information in the performance of their duties or activities for NSF.

8. Audit. Information from a system may be disclosed to government agencies and other entities authorized to perform audits, including financial and other audits, of the agency and its activities.

9. Law Enforcement. Information from a system may be disclosed, where the information indicates a violation or potential violation of civil or criminal law, including any rule, regulation or order issued pursuant thereto, to appropriate Federal, State, or local agencies responsible for investigating, prosecuting, enforcing, or implementing such statute, rule, regulation, or order.

10. Disclosure When Requesting Information. Information from a system may be disclosed to Federal, State, or local agencies which maintain civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

11. To the news media and the public when: (1) a matter has become public knowledge, (2) the NSF Office of the Director determines that disclosure is

necessary to preserve confidence in the integrity of NSF or is necessary to demonstrate the accountability of NSF's officers, employees, or individuals covered by this system, or (3) the Office of the Director determines that there exists a legitimate public interest in the disclosure of the information, except to the extent that the Office of the Director determines in any of these situations that disclosure of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

In addition to the above standard NSF routine uses, the following routine uses apply to this system, *i.e.,* records may also be disclosed:

To the awardee institution or other institution(s) or organization(s) subject to investigation in order to gather information necessary for the agency, law enforcement officials, and/or other authorized authorities to make a compliance determination with respect to the complaint allegations or to conduct compliance monitoring in connection with a resolution agreement.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic form, including electronic storage media, and may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage. In the conduct of agency business, copies may also be printed or maintained in paper format.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be maintained by the subject individual's name and retrieved by personally assigned identifier, such as case tracking number. If a subject individual authorizes a third-party individual to file a complaint or report on the subject individual's behalf, such records will be maintained and retrieved by the same assigned case tracking number or other identifier. Records in this system are not maintained or retrieved by the name or other personally assigned identifier of any third-party individuals who may be identified in such system records (*e.g.,* witnesses, individuals engaged in the alleged conduct).

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records will be maintained and destroyed in accordance with applicable records schedules issued or approved by NARA.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable Federal law, rules, and policies, including all applicable NSF automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties. All users are required to take annual NSF IT Security and Privacy Awareness Training, which covers the procedures for handling Controlled Unclassified Information (CUI), including personally identifiable information (PII) subject to the Privacy Act of 1974. Electronic records are maintained in a secure password-protected environment. Permission-level assignments will allow internal agency users access only to those functions for which they are authorized. Paper copies, if any, of system records are maintained in secure, access-controlled areas or buildings, and stored in a locked drawer, behind a locked door, or at a secure offsite location.

RECORD ACCESS PROCEDURES:

Individuals seeking to access records about themselves in this system must follow the procedures found at 45 CFR part 613 (NSF Privacy Act Regulations). Individuals who register and create a user account to file a complaint or report in the system may access status information or certain other system data pertaining to their complaint without the need to file a formal written Privacy Act access request under 45 CFR part 613.

CONTESTING RECORD PROCEDURES:

Follow the procedures found at 45 CFR part 613. Individuals who register and create a user account in the system to file a complaint in the system may access and update or modify certain system records pertaining to their complaint without the need to file a formal written Privacy Act amendment request under 45 CFR part 613.

NOTIFICATION PROCEDURES:

See 45 CFR part 613.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

NSF–85

SYSTEM NAME AND NUMBER:

NSF–85, Reasonable Accommodation Request E-Filing System.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

U.S. National Science Foundation (NSF), 401 Dulany Street, Alexandria, VA 22314. Records may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

29 U.S.C. 791 *et seq.;* 42 U.S.C. 2000e *et seq.;* 42 U.S.C. 12101 *et seq.;* E.O. 11478; E.O. 13164; 29 CFR parts 1605, 1614, and 1630.

PURPOSE(S) OF THE SYSTEM:

This system is maintained for the purpose of receiving, considering, deciding, and implementing requests for reasonable accommodation made by NSF employees, applicants for NSF employment, and other individuals conducting business at NSF.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

NSF employees, applicants for employment, and other individuals conducting business at NSF who have requested a reasonable accommodation under applicable Federal law, regulation, and policy.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include, but are not limited to, user account and profile data (*e.g.,* name, email address, phone), requests for reasonable accommodation and supporting documents, information concerning the nature of the disability or other reason for the requested accommodation, medical records or other substantiating documentation, notes or records made during evaluation of such requests, including the agency's determination on the request, requests for reconsideration or internal agency appeals; and disposition of all requests and appeals.

RECORD SOURCE CATEGORIES:

Individuals requesting a reasonable accommodation; NSF managers, supervisors, or staff, where applicable; health care providers or others requested to provide supporting documentation.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The following NSF standard routine uses apply:

1. Members of Congress. Information from a system may be disclosed to congressional offices in response to inquiries from the congressional offices made at the request of the individual to whom the record pertains.

2. Freedom of Information Act/ Privacy Act Compliance. Information from a system may be disclosed to the Department of Justice or the Office of Management and Budget to obtain advice regarding NSF's obligations under the Freedom of Information Act and the Privacy Act.

3. Counsel. Information from a system may be disclosed to NSF's legal representatives, including the Department of Justice and other outside counsel, where the agency is a party in litigation or has an interest in litigation and the information is relevant and necessary to such litigation, including when any of the following is a party to the litigation or has an interest in such litigation: (a) NSF, or any component thereof; (b) any NSF employee in his or her official capacity; (c) any NSF employee in his or her individual capacity, where the Department of Justice has agreed to, or is considering a request to, represent the employee; or (d) the United States, where NSF determines that litigation is likely to affect the agency or any of its components.

4. National Archives and Records Administration (NARA). Information from a system may be disclosed to representatives of NARA during records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

5. Response to an Actual or Suspected Compromise or Breach of Personally Identifiable Information. NSF may disclose information from the system:

a. to appropriate agencies, entities, and persons when (1) NSF suspects or has confirmed that there has been a breach of the system of records; (2) NSF has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NSF (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 NSF's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

b. to another Federal agency or Federal entity, when NSF 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.

6. Courts. Information from a system may be disclosed to the Department of Justice or other agencies in the event of a pending court or formal administrative proceeding, when the information is relevant and necessary to that proceeding, for the purpose of representing the government, or in the course of presenting evidence, or the information may be produced to parties or counsel involved in the proceeding in the course of pre-trial discovery.

7. Contractors. Information from a system may be disclosed to contractors, agents, experts, consultants, or others performing work on a contract, service, cooperative agreement, job, or other activity for NSF and who have a need to access the information in the performance of their duties or activities for NSF.

8. Audit. Information from a system may be disclosed to government agencies and other entities authorized to perform audits, including financial and other audits, of the agency and its activities.

9. Law Enforcement. Information from a system may be disclosed, where the information indicates a violation or potential violation of civil or criminal law, including any rule, regulation or order issued pursuant thereto, to appropriate Federal, State, or local agencies responsible for investigating, prosecuting, enforcing, or implementing such statute, rule, regulation, or order.

10. Disclosure When Requesting Information. Information from a system may be disclosed to Federal, State, or local agencies which maintain civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

11. To the news media and the public when: (1) a matter has become public knowledge, (2) the NSF Office of the Director determines that disclosure is necessary to preserve confidence in the integrity of NSF or is necessary to demonstrate the accountability of NSF's officers, employees, or individuals covered by this system, or (3) the Office of the Director determines that there exists a legitimate public interest in the disclosure of the information, except to the extent that the Office of the Director determines in any of these situations that disclosure of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

In addition to the above standard NSF routine uses, the following routine uses apply to this system, *i.e.,* records may also be disclosed:

12. To an authorized appeal grievance examiner, formal complaints examiner, administrative judge, equal employment opportunity investigator, arbitrator or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by the individual requesting the accommodation.

13. To first aid and safety personnel, when appropriate, if the disability might require emergency treatment;

14. To Federal Government officials or any of their assignees charged with the responsibility of investigating NSF's compliance with the Rehabilitation Act of 1973, as amended, or other applicable authorities.

15. To the U.S. Office of Management and Budget (OMB), Department of Labor (DOL), Office of Personnel Management (OPM), Equal Employment Opportunity Commission (EEOC), or Office of Special Counsel (OSC) to obtain advice regarding statutory, regulatory, policy, and other requirements related to reasonable accommodation.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic form, including electronic storage media, and may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage. In the conduct of agency business, copies may also be printed or maintained in paper format.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be maintained by the subject individual's name and retrieved by personally assigned identifier, such as case tracking number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records will be maintained and destroyed in accordance with applicable records schedules issued or approved by NARA. See, *e.g.,* General Records Schedule 2.3, Item 020 (reasonable or religious accommodation case files).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable Federal law, rules, and policies, including all applicable NSF automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties. All users are required to take annual NSF IT Security and Privacy Awareness Training, which covers the procedures for handling Controlled Unclassified Information (CUI), including personally identifiable information (PII) subject to the Privacy Act of 1974. Electronic records are maintained in a secure password-protected environment. Permission-level assignments will allow internal agency users access only to those functions for which they are authorized. Paper copies, if any, of system records are maintained in secure, access-controlled areas or buildings, and stored in a locked drawer, behind a locked door, or at a secure offsite location.

RECORD ACCESS PROCEDURES:

Individuals seeking to access records about themselves in this system must follow the procedures found at 45 CFR part 613 (NSF Privacy Act Regulations). Individuals who register and create a user account to file a reasonable accommodation in the system may access status or certain other information about their request directly from the system, without the need to file a formal written Privacy Act access request under 45 CFR part 613.

CONTESTING RECORD PROCEDURES:

Follow the procedures found at 45 CFR part 613.

NOTIFICATION PROCEDURES:

See 45 CFR part 613.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

NSF–86

SYSTEM NAME AND NUMBER:

NSF–86, Sexual Assault and Harassment Prevention and Response Program (SAHPR) Case Management Tracking System.

SECURITY CLASSIFICATION:

Unclassified.

SYSTEM LOCATION:

U.S. National Science Foundation (NSF), 401 Dulany Street, Alexandria, VA 22314. Records may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

5 U.S.C. 2302(b); 29 U.S.C. 206(d); 29 U.S.C. 621 *et seq.;* 29 U.S.C. 791; 42 U.S.C. 1861 *et seq.;* 42 U.S.C. 2000e–16 *et seq.;* 42 U.S.C. 2000ff *et seq.;* 42 U.S.C. 12101 *et seq.;* Pub. L. 107–174, as amended; E.O. 11478; E.O. 14021; 2 CFR 200.300 and 200.303; and other authorities, as applicable.

PURPOSE(S) OF THE SYSTEM:

To log, track, and coordinate the agency's response to reported incidents of sexual assault, harassment and stalking in NSF-funded programs and activities, and other inquiries received through the SAHPR program office; to provide information (*e.g.,* about available support resources or training); to make referrals to appropriate officials, agencies, and entities; to enhance compilation and accuracy of statistical data and management reports; to assess the program's effectiveness; to help develop or update procedures and training; or to recommend other action by the agency or others to help prevent alleged sexual assault, sexual harassment, and stalking, as applicable.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The system covers individuals who have formally reported to NSF's Office of the Inspector General or other investigative entity that they were the alleged victim or target of sexual assault, sexual harassment or stalking, or who have been identified as an alleged victim or target in a report filed with the investigative entity by a third party. The system also covers other individuals who may directly contact the SAHPR program office for information on how or where to report sexual assault, sexual harassment or stalking or for other information or support services relating to such incidents in NSF-funded programs and activities. Covered individuals may include, but are not limited to, NSF employees, contractors, participants in research or infrastructure projects or operations funded by an NSF award.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records may include, but are not limited to, name, email address, and/or other contact information of the individual identified as an alleged victim or target of sexual assault, harassment, or stalking in a formal report with NSF's Office of Inspector General or other investigative entity, or individuals who directly contact the SAHPR program office; date that the inquiry was received; date the case record was initially created in the system; assigned case number; type of incident; location (site) of incident; information regarding third parties, as applicable (*e.g.,* alleged offender(s), witness(es)); notes regarding the program office's handling or disposition of the matter (*e.g.,* informational response, referral, related investigational case numbers).

RECORD SOURCE CATEGORIES:

Individuals who contact the SAHPR program office regarding the alleged incident; reports filed by the subject individual or third-party individuals (*e.g.,* witnesses) with NSF's Office of Inspector General or other entities (*e.g.,* the impacted individual's institution, law enforcement).

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:

The following NSF standard routine uses apply:

1. Members of Congress. Information from a system may be disclosed to congressional offices in response to inquiries from the congressional offices made at the request of the individual to whom the record pertains.

2. Freedom of Information Act/ Privacy Act Compliance. Information from a system may be disclosed to the Department of Justice or the Office of Management and Budget to obtain advice regarding NSF's obligations under the Freedom of Information Act and the Privacy Act.

3. Counsel. Information from a system may be disclosed to NSF's legal representatives, including the Department of Justice and other outside counsel, where the agency is a party in litigation or has an interest in litigation and the information is relevant and necessary to such litigation, including when any of the following is a party to the litigation or has an interest in such litigation: (a) NSF, or any component thereof; (b) any NSF employee in his or her official capacity; (c) any NSF employee in his or her individual capacity, where the Department of Justice has agreed to, or is considering a request to, represent the employee; or (d) the United States, where NSF determines that litigation is likely to affect the agency or any of its components.

4. National Archives and Records Administration (NARA). Information

from a system may be disclosed to representatives of NARA during records management inspections conducted under the authority of 44 U.S.C. 2904 and 2906.

5. Response to an Actual or Suspected Compromise or Breach of Personally Identifiable Information. NSF may disclose information:

a. to appropriate agencies, entities, and persons when (1) NSF suspects or has confirmed that there has been a breach of the system of records; (2) NSF has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, NSF (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 NSF's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

b. to another Federal agency or Federal entity, when NSF 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.

6. Courts. Information from a system may be disclosed to the Department of Justice or other agencies in the event of a pending court or formal administrative proceeding, when the information is relevant and necessary to that proceeding, for the purpose of representing the government, or in the course of presenting evidence, or the information may be produced to parties or counsel involved in the proceeding in the course of pre-trial discovery.

7. Contractors. Information from a system may be disclosed to contractors, agents, experts, consultants, or others performing work on a contract, service, cooperative agreement, job, or other activity for NSF and who have a need to access the information in the performance of their duties or activities for NSF.

8. Audit. Information from a system may be disclosed to government agencies and other entities authorized to perform audits, including financial and other audits, of the agency and its activities.

9. Law Enforcement. Information from a system may be disclosed, where the information indicates a violation or potential violation of civil or criminal law, including any rule, regulation or order issued pursuant thereto, to appropriate Federal, State, or local agencies responsible for investigating, prosecuting, enforcing, or implementing such statute, rule, regulation, or order.

10. Disclosure When Requesting Information. Information from a system may be disclosed to Federal, State, or local agencies which maintain civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary, to obtain information relevant to an agency decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

11. To the news media and the public when: (1) a matter has become public knowledge, (2) the NSF Office of the Director determines that disclosure is necessary to preserve confidence in the integrity of NSF or is necessary to demonstrate the accountability of NSF's officers, employees, or individuals covered by this system, or (3) the Office of the Director determines that there exists a legitimate public interest in the disclosure of the information, except to the extent that the Office of the Director determines in any of these situations that disclosure of specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

In addition to the above standard NSF routine uses, the following routine uses apply to this system, *i.e.,* records may also be disclosed:

12. To other appropriate non-NSF officials, agencies, or entities in order to investigate the alleged sexual harassment or to take action to address the matter. In such cases, the SAHPR program office may obtain the individual's written consent before making such a referral.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic form, including electronic storage media, and may also be electronically maintained in remote locations by NSF or contractors on behalf of NSF, including in cloud storage. In the conduct of agency business, copies may also be printed or maintained in paper format.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Records may be maintained by the subject individual's name and retrieved by personally assigned identifier, such as case tracking number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records will be maintained and destroyed in accordance with applicable records schedules issued or approved by NARA. *See, e.g.,* General Records Schedule 2.3, Item 050 (harassment complaint case files).

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Records in this system are safeguarded in accordance with applicable Federal law, rules, and policies, including all applicable NSF automated systems security and access policies. Strict controls have been imposed to minimize the risk of compromising the information that is being stored. Access to the computer system containing the records in this system is limited to those individuals who have a need to know the information for the performance of their official duties. All users are required to take annual NSF IT Security and Privacy Awareness Training, which covers the procedures for handling Controlled Unclassified Information (CUI), including personally identifiable information (PII) subject to the Privacy Act of 1974. Electronic records are maintained in a secure password-protected environment. Permission-level assignments will allow internal agency users access only to those functions for which they are authorized. Paper copies, if any, of system records are maintained in secure, access-controlled areas or buildings, and stored in a locked drawer, behind a locked door, or at a secure offsite location.

RECORD ACCESS PROCEDURES:

Individuals seeking to access records about themselves in this system must follow the procedures found at 45 CFR part 613 (NSF Privacy Act Regulations).

CONTESTING RECORD PROCEDURES:

Follow the procedures found at 45 CFR part 613.

NOTIFICATION PROCEDURES:

See 45 CFR part 613.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None.

HISTORY:

None.

Thomas A. Boger,

Acting Senior Agency Official for Privacy, U.S. National Science Foundation.

[FR Doc. 2026–22540 Filed 11–4–26; 8:45 am]

BILLING CODE 7555–01–P