SMALL BUSINESS ADMINISTRATION

Privacy Act of 1974; System of Records

AGENCY: U.S. Small Business Administration.

ACTION: Notice of New Privacy Act System of Records.

SUMMARY: The Small Business Administration (SBA) proposes to add a new system of records titled, Insider Threat Program System of Records, to its inventory of records systems subject to the Privacy Act of 1974 (5 U.S.C. 552a), as amended. Publication of this notice complies with the Privacy Act and the Office of Management and Budget (OMB) Circular A-130 requirement for agencies to publish a notice in the Federal Register whenever the agency establishes a new System of Records.

DATES: This action will be effective without further notice on **[INSERT DATE 45 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** unless comments are received that would result in a contrary determination.

ADDRESSES: Submit written comments to Joseph P. Loddo, Director, Office of Continuous Operations and Risk Management, U.S. Small Business Administration, 409 3rd Street SW, 5th Floor, Washington, DC 20416.

FOR FURTHER INFORMATION CONTACT: Joseph P. Loddo, (202) 205-7014.

SUPPLEMENTARY INFORMATION:

A System of Records is a group of any records under the control of a Federal agency from which information is retrieved by the name of an individual or by a number, symbol or other identifier assigned to the individual. The Privacy Act, 5 U.S.C. 552a, requires each Federal agency to publish in the Federal Register a System of Records notice (SORN) identifying and describing each System of Records the agency maintains, the

purposes for which the agency uses the personally identifiable information (PII) in the system, the routine uses for which the agency discloses such information outside the agency, and how individuals can exercise their rights related to their PII information.

The U.S. Small Business Administration has created an Agency-wide repository known as the Insider Threat Program System of Records to manage insider threat matters within the SBA. The Insider Threat Program was mandated by E.O. 13587, Responsible Sharing and Safeguarding of Classified Information," issued October 7, 2011, which requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified and controlled unclassified information with appropriate protections for privacy and civil liberties. Insider threats include: Attempted or actual espionage, subversion, sabotage, terrorism, or extremist activities: unauthorized use of or intrusion into automated information systems; unauthorized disclosure of classified, controlled unclassified, sensitive, or proprietary information or technology; and indicators of potential insider threats. The SBA Insider Threat Program repository relies upon existing information from any SBA office, program, record, or source, and may include records from information security, personnel security, and systems security to support insider threat investigations. The SBA is not implementing a new IT system for the insider threat program.

SYSTEM NAME: Insider Threat Program System of Records Notice

SYSTEM CLASSIFICATION: Unclassified

SYSTEM LOCATION: SBA headquarters (HQ) and all SBA field offices and centers

SYSTEM MANAGER(S): Joseph Loddo, Director, Office of Continuous Operations and Risk Management, 409 3rd Street SW, Washington DC, 20416**.**

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108-458; Intelligence Authorization Act for FY 2010, Pub. L. 111-259; Atomic Energy Act of 1954, 60 Stat. 755, August 1, 1946; Title 6 U.S.C. 341(a)(6), 28 U.S. Code § 535, Investigation of Crimes Involving Government Employees Limitations; Title 40 U.S.C. 1315, Title 50 U.S.C. 3381, Coordination of Counterintelligence Activities; E.O. 10450, Security Requirements for Government Employment, April 17, 1953; E.O. 12333, United States Intelligence Activities (as amended); E.O. 12829, National Industrial Security Program; E.O. 12968, Access to Classified Information, August 2, 1995; E.O. 13467, Reforming Processes Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified National Security Information, June 30, 2008; E.O. 13488, Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust, January 16, 2009; E.O. 13526, Classified National Security Information; E.O. 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, October 7, 2011; and Presidential Memorandum National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs, November 21, 2012

PURPOSE OF THE SYSTEM:

The purpose of the Insider Threat Program System of Records is to manage insider threat matters; facilitate insider threat investigations and activities associated with counterintelligence and counterespionage complaints, inquiries, and investigations; identify threats to SBA resources and information assets; track referrals of potential

insider threats to internal and external partners; and provide statistical reports and meet other insider threat reporting requirements.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM INCLUDE:

- SBA current or former employees, contractors, or detailed staff who have or had access to classified and sensitive unclassified information or information systems.
- Other individuals, including government personnel and private sector individuals, who are authorized by SBA to access Agency facilities, communications security equipment, and/or information technology systems that process sensitive or classified national security information, and controlled unclassified information.
- Family members, dependents, relatives, and individuals with a personal association to an individual who is the subject of an insider threat investigation; and
- Witnesses and other individuals who provide statements or information to SBA related to an insider threat inquiry.

CATEGORIES OF RECORDS IN THE SYSTEM:

Records will be created and maintained on a limited basis, as a result of a reported issue requiring analysis and consideration by the insider threat HUB.

Categories of Records in the system may include:

- Individual's name;
- Date and place of birth;
- Social Security Number;
- Address;
- Publicly available social media account information;

- Personal and official email address;
- Personal and official phone number;
- Work History;
- Information on family members, dependents, relatives, and other personal associations;
- Passport numbers;
- Gender;
- Hair and eye color;
- Other physical or distinguishing attributes or an individual;
- Medical reports;
- Access control pass, or other identifying number, and
- Photographic images, videotapes, voiceprints, or DVDs;

Reports of investigation regarding security violations, including but not limited to:

- 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;

Any information related to the management and operation of specific investigations and the overall SBA insider threat program, including but not limited to:

- Documentation pertaining to investigative or analytical efforts by SBA insider threat program personnel to identify threats to SBA personnel, property, facilities, and information;
- Records collated to examine information technology events and other information that could reveal potential insider threat activities;
- Travel records;
- Intelligence reports and database query results relating to individuals covered by this system;
- Information obtained from the Intelligence Community, the Federal Bureau of Investigation (FBI), 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 but not limited to espionage or unauthorized disclosures of classified national security information;
- Information provided by record subjects and individual members of the public; and
- Information provided by individuals who report known or suspected insider threats.

RECORD SOURCE CATEGORIES:

After events are identified for insider threat HUB consideration, relevant records are obtained from Department officials, employees, contractors, and other individuals who are associated with or represent SBA; officials from other foreign, Federal, tribal, State,

and local government organizations; non-government, commercial, public, and private agencies and organizations; relevant SBA records, databases, and files, including personnel security files, facility access records, security incidents or violation files, network security records, investigatory records, visitor records, travel records, foreign visitor or contact reports, and financial disclosure reports; media, including periodicals, newspapers, and broadcast transcripts; intelligence source documents; publicly available information, including publicly available social media; and complainants, informants, suspects, and witnesses.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside SBA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

A. To the Department of Justice (DOJ), including offices of the U.S. Attorneys, or other Federal agency conducting litigation or in proceedings before any court, adjudicative, or administrative body, when it is relevant or necessary to the litigation or has an interest in such litigation:

1. Any employee or former employee of SBA in his or her official capacity;
2. Any employee or former employee of SBA in his or her individual capacity when DOJ or SBA has agreed to represent the employee; or
3. The United States or any agency thereof.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration (NARA) or General Services Administration (GSA) pursuant to records management inspections being conducted under the authority of 44 U.S.C. 2904 and 2906.

D. To an agency or organization for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when:

1. SBA suspects or has confirmed that the security or confidentiality of information processed and maintained by the SBA has been compromised.

2. SBA has determined that as a result of the suspected or confirmed compromise, there is a risk of identity theft or fraud, harm to economic or property interests, harm to an individual, or harm to the security or integrity of this system or other systems or programs (whether maintained by SBA or another agency or entity) that rely upon the compromised information; and

3. The disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with SBA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contact, service, grant, cooperative agreement, or other assignment for SBA, when necessary to accomplish an agency function related to this System of

Records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to SBA employees.

G. To an appropriate Federal, State, tribal, territorial, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. 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 SBA 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.

I. To an individual's prospective or current employer to the extent necessary to determine employment eligibility.

J. To third parties during the course of an investigation to the extent necessary to obtain information pertinent to the investigation, provided disclosure is appropriate to the proper performance of the official duties of the individual making the disclosure.

K. To a public or professional licensing organization when such information indicates, either by itself or in combination with other information, a violation or potential violation of professional standards, or reflects on the moral, educational, or professional qualifications of an individual who is licensed or who is seeking to become licensed.

L. To another Federal agency in order to conduct or support authorized counterintelligence activities, as defined by 50 U.S. C. 3003(3).

M. To any Federal, State, local, tribal, territorial, foreign, or multinational government or agency, or appropriate private sector individuals and organizations lawfully engaged in national security or homeland defense for that entity's official responsibilities, including responsibilities to counter, deter, prevent, prepare for, respond to, threats to national or homeland security, including an act of terrorism or espionage.

N. To a Federal, State, local, tribal, territorial, government or agency lawfully engaged in the collection of intelligence (including national intelligence, foreign intelligence, and counterintelligence), counterterrorism, homeland security, law enforcement or law enforcement intelligence, and other information, when disclosure is undertaken for intelligence, counterterrorism, homeland security, or related law enforcement purposes, as authorized by U.S. law or E.O.

O. To any individual, organization, or entity, as appropriate, to notify them of a serious threat to homeland security for the purpose of guarding them against or responding to such a threat, or when there is a reason to believe that the recipient is or could become the target of a particular threat, to the extent the information is relevant to the protection of life, health, or property.

P. To members of the U.S. House Committee on Oversight and Government Reform and the Senate Homeland Security and Governmental Affairs Committee pursuant to a written request under 5 U.S.C. 2954, after consultation with the Privacy Act Officer and the General Counsel.

Q. To individual members of the Senate Select Committee on Intelligence and the House Permanent Select Committee for intelligence in connection with the exercise of the Committees' oversight and legislative functions, when such disclosures are necessary to a lawful activity of the United States, after consultation with the Privacy Act Officer and the General Counsel.

R. To a Federal agency or entity that has information relevant to an allegation or investigation regarding an insider threat matter, or to a federal agency or entity that was consulted during the processing of the allegation or investigation but that did not ultimately have relevant information.

S. To a former SBA employee, SBA contractor, or individual sponsored by SBA for a security clearance for purposes of responding to an official inquiry by Federal, State, local, tribal, or territorial government agencies or professional licensing authorities; or facilitating communications with a former employee that may be relevant and necessary for personnel-related or other official purposes when SBA requires information or consultation assistance from the former employees regarding a matter within that person's former area of responsibility.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Insider Threat Program stores records for each evaluated event in a central repository within the SBA internal network. The records may be stored on digital media.

POLICIES AND PRACTICIES FOR RETRIEVAL OF RECORDS:

SBA may retrieve records by first and last name, Social Security number, date of birth, phone number, other unique individual identifiers, and other types of information by keyword search.

POLICIES AND PRACTICIES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are maintained in accordance with SBA SOP 00 41 2. Records maintained as part of the General Records Schedules (GRS) are disposed of accordingly.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

SBA safeguards records in this repository according to applicable rules and policies, including all applicable SBA automated systems security and access policies. Access to the repository or other storage systems containing the records in this system is limited to to individuals who have the appropriate clearances or permissions and who have a need to know the information in order to perform their official duties. The Agency should consider storing Insider Threat records on a stand-alone computer in order to reduce risk of unauthorized access.

RECORD ACCESS PROCEDURES:

Access and use is limited to persons with official need to know; computers are protected by access control mechanisms. Users are evaluated on a recurring basis to ensure need-to-know still exists.

RECORD ACCESS PROCEDURES:

Systems Manager will determine procedures.

CONTESTING RECORD PROCEDURES:

Notify officials listed above and state reason(s) for contesting any information and provide proposed amendment(s) sought.

NOTIFICATION PROCEDURE:

Individuals may make record inquiries in person or in writing to the Systems Manager. When seeking records about yourself from this System of Records or any other Departmental System of Records, your request must conform with the Privacy Act regulations set forth in 6 CFR part 5; Disclosure of Records and Information. You must first verify your identity, meaning that you must provide your full name, current address, and date and place of birth. You must sign your request, and your signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization.

- Explain why you believe the Agency would have information on you;
- Specify when you believe the records would have been created; and
- Provide any other information that will help the Agency locate the requested records.

Without the above information, the Agency may not be able to conduct an effective search, and your request may be denied due to lack of specificity or lack of compliance with applicable regulations.

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

None

Dated: June 19, 2018.

Joseph P. Loddo,

Director, Office Continuous Operations and Risk Management,

Senior Insider Threat Program Official.

[FR Doc. 2018-14209 Filed: 7/2/2018 8:45 am; Publication Date: 7/3/2018]