[Billing Code 7709-02-P]

PENSION BENEFIT GUARANTY CORPORATION

Privacy Act of 1974; System of Records

AGENCY: Pension Benefit Guaranty Corporation.

ACTION: Notice of a new system of records.

SUMMARY: The Pension Benefit Guaranty Corporation (PBGC) is proposing the following changes to its system of records notices to establish a new system of records PBGC-26: PBGC Insider Threat and Data Loss Prevention. The new system of records will cover records about individuals, retrieved by personal identifier, which are compiled and used by PBGC's Insider Threat and Data Loss Prevention teams, to administer PBGC's insider threat and data loss prevention programs. Because records in this system include investigatory material compiled for law enforcement purposes, elsewhere in this issue of the Federal Register PBGC has published a final rule to exempt this system of records from certain requirements of the Privacy Act. The system of records is more fully described in in the **SUPPLEMENTARY INFORMATION** section of this notice and in the System of Records Notice (SORN) published in this notice.

DATES: Comments must be received on or before [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE *FEDERAL REGISTER*]. The system of records described herein will become effective [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*], without further notice, unless comments result in a contrary determination and a notice is published to that effect.

ADDRESSES: You may submit written comments to PBGC by any of the following methods:

- Federal eRulemaking Portal: http://www.regulations.gov. Follow the website

instructions for submitting comments.

- E-mail: reg.comments@pbgc.gov. Refer to SORN in the subject line.
- Mail or Hand Delivery: Regulatory Affairs Division, Office of the General Counsel, Pension Benefit Guaranty Corporation, 1200 K Street, NW, Washington, DC 20005-4026.

All submissions must include the agency's name (Pension Benefit Guaranty Corporation, or PBGC) and refer to "SORN." All comments received will be posted without change to PBGC's website, www.pbgc.gov, including any personal information provided. Copies of comments may also be obtained by writing to Disclosure Division, Office of the General Counsel, Pension Benefit Guaranty Corporation, 1200 K Street, NW, Washington, DC 20005-4026, or calling 202-326-4040 during normal business hours. (TTY users may call the Federal relay service toll-free at 1-800-877-8339 and ask to be connected to 202-326-4040.)

FOR FURTHER INFORMATION CONTACT: Margaret Drake, Chief Privacy Officer, Pension Benefit Guaranty Corporation, Office of the General Counsel, 1200 K Street NW, Washington, DC 20005, 202-326-4400, extension 6435. For access to any of PBGC's system of records, contact D. Camilla Perry, Disclosure Officer, Office of the General Counsel, Disclosure Division, 1200 K Street NW, Washington DC 20005, or by calling 202-326-4040.

SUPPLEMENTARY INFORMATION: PBGC is proposing to establish a new system of records titled, "PBGC-26, PBGC Insider Threat and Data Loss Prevention – PBGC." Executive Order 13587, issued on October 7, 2011, mandated that agencies with classified networks establish insider threat programs. While PBGC does not have any classified networks, it does maintain a significant amount of Controlled Unclassified Information (CUI) that, under law, it is required to safeguard from unauthorized access or disclosure. One method utilized by PBGC to

ensure that only those with a need-to-know have access to CUI is a set of tools to minimize data loss, whether inadvertent or intentional.

Working from the Minimum Standards set forth in the Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012), PBGC is also establishing an Insider Threat Program. While PBGC is not legally mandated to deploy an insider threat program, the principles developed by the National Institute of Standards and Technology and the National Insider Threat Task Force "can also be employed effectively to improve the security of Controlled Unclassified Information in non-national security systems." An "insider" is any individual authorized to access PBGC facilities, information, equipment, and systems. This includes Federal employees and contractors. An "insider threat" occurs when that individual exceeds their authorized access, intentionally or not, or uses information for an improper purpose, including, but not limited to, personal gain, which "negatively affect[s] the confidentiality, integrity, or availability" of PBGC data.

The records that PBGC will compile to administer its data loss prevention and insider threat programs may be from any PBGC program, record, or source, and may contain records pertaining to information security, personnel security, or physical security. The records covered under PBGC-26,PBGC Insider Threat and Data Loss Prevention – PBGC, include investigatory material compiled for law enforcement purposes. Accordingly, PBGC has published a Final Rule in the Federal Register to exempt such material in the new system or record from certain requirements under the Privacy Act of 1974 (5 U.S.C. 552a), based on subsection (k)(2) of the Act.

The collection and maintenance of these records is new. The implementation of this new system of records will be effective on [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

Issued in Washington, DC.

Gordon Hartogensis,
Director,
Pension Benefit Guaranty Corporation.

SYSTEM NAME AND NUMBER:

PBGC – 26: PBGC Insider Threat and Data Loss Prevention — PBGC

SECURITY CLASSIFICATION:

Unclassified

SYSTEM LOCATION:

Pension Benefit Guaranty Corporation (PBGC), 1200 K Street NW, Washington, DC 20005. (Records may be kept at an additional location as backup for continuity of operations.)

SYSTEM MANAGER(S) AND ADDRESS:

Chief Information Officer, Office of Information Technology, PBGC, 1200 K Street, NW, Washington, DC 20005.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

29 U.S.C. 1302(b)(3); 5 U.S.C. 301; 44 U.S.C. 3101; 44 U.S.C. 3554; Executive Order 13587, Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information (Oct. 7, 2011); Presidential Memorandum – National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs (Nov. 21, 2012); Executive Orders 13488 and 13467, as amended by 13764, To Modernize the Executive Branch-Wide Governance Structure and Processes for Security Clearances, Suitability and Fitness for Employment, and Credentialing, and Related Matters; Executive Order 3356, Controlled Unclassified Information (Nov. 4, 2010); 5 CFR part 731; 5 CFR part 302; OMB Circular A-130 (July 28, 2016); National Institute of Standards and Technology Special Publication 800-53.

PURPOSE(S) OF THE SYSTEM:

The purpose of the system is to detect anomalous behavior by PBGC insiders and, as warranted, gather information from sources or existing PBGC systems of records to support an investigation of the incident.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

The categories of individuals covered by this system are PBGC insiders, defined as any person with authorized access to any PBGC resource including facilities, information, equipment, networks, or systems.

CATEGORIES OF RECORDS IN THE SYSTEM:

A. The system will contain these categories of records:

Information collected through user activity monitoring, including keystrokes, screen captures, and content transmitted via email, chat, or data import or export.

Reports of investigation regarding security violations and privacy breaches, including incident reports; usernames and aliases, levels of network access, audit data, information regarding misuse of PBGC devices, information regarding unauthorized use of removable media, and logs of printer, copier, and facsimile machine use.

Records relating to the management and operation of PBGC personnel and physical security, including information relating to continued eligibility for access to PBGC facilities, information, and information systems.

Information identifying threats to PBGC personnel, property, facilities, and information; information obtained from the Department of Justice, 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 personally identifiable information (PII).

B. The system may include these categories of records:

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.

Reports furnished to the PBGC, or collected by PBGC, in connection with personnel security investigations and Insider Threat Detection Program operated by PBGC pursuant to Federal laws and Executive Orders, rules, regulations, guidance, and PBGC policies.

Documentation pertaining to investigative or analytical efforts by PBGC Insider Threat Program Personnel to identify threats to PBGC personnel, property, facilities, and information.

Intelligence reports and database query results relating to individuals covered by this system.

RECORD SOURCE CATEGORIES:

To monitor for, identify, and respond to potential insider threats, information in the system will be received on an as needed basis from PBGC employees, contractors, vendors, interns, and detailees; 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; PBGC human resources databases and files; PBGC contractor files; PBGC's Office of Information Technology; information collected through user activity monitoring; PBGC 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 THE PURPOSES OF SUCH USES:

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 522a(b), and:

1. General Routine Uses G1 through G14 apply to this system of records (see Prefatory Statement of General Routine Uses).

2. Records may be disclosed to any person, organization, or governmental entity in order to notify them of a serious threat for the purpose of guarding against or responding to the threat.

3. 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 emended, 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.

4. Records may be disclosed to the U.S. Department of Homeland Security (DHS) if captured in an intrusion detection system used by PBGC 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.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Records are maintained in electronic form (including computer databases or discs). Records may also be maintained on back-up tapes, or on a PBGC or a contractor-hosted network.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:

Information from this system may be retrieved by numerous data elements and key word searches, including, but not limited to name, dates, subject, and other information retrievable with full text searching capability.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

PBGC has established security and privacy protocols that meet the required security and privacy standards issued by the National Institute of Standards and Technology (NIST). Records are maintained in a secure, password protected electronic system that utilizes security hardware and software to include multiple firewalls, active intruder detection, and role-based access controls. PBGC has adopted appropriate administrative, technical, and physical controls in accordance with PBGC's security program to protect the confidentiality, integrity, and availability of the information, and to ensure that records are not disclosed to or accessed by unauthorized individuals.

Electronic records are stored on computer networks, which may include cloud-based systems, and protected by controlled access with Personal Identity Verification (PIV) cards, assigning user accounts to individuals needing access to the records and by passwords set by authorized users that must be changed periodically.

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 210, 220, 230, and 240.

RECORD ACCESS PROCEDURES:

Individuals, or third parties with written authorization from the individual, wishing to request access to their records in accordance with 29 CFR 4902.4, should submit a written request to the Disclosure Officer, PBGC, 1200 K Street, NW, Washington, DC 20005, providing their name, address, date of birth, and verification of their identity in accordance with 29 CFR 4902.3(c).

CONTESTING RECORD PROCEDURES:

Individuals, or third parties with written authorization from the individual, wishing to amend their records must submit a written request identifying the information they wish to correct in their file, in addition to following the requirements of the Record Access Procedure above.

NOTIFICATION PROCEDURES:

Individuals, or third parties with written authorization from the individual, wishing to learn whether this system of records contains information about them should submit a written request to the Disclosure Officer, PBGC, 1200 K Street, NW, Washington, DC 20005, providing their name, address, date of birth, and verification of their identity in accordance with 29 CFR 4902.3(c).

EXEMPTIONS PROMULGATED FOR THE SYSTEM:

Pursuant to 5 U.S.C. 552a(k)(2), PBGC has established regulations at 29 CFR 4902.12 that exempt records in this system depending on their purpose.

HISTORY:

None.

[FR Doc. 2019-14605 Filed: 7/8/2019 8:45 am; Publication Date: 7/9/2019]