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 C.F.R. 731; 5 C.F.R. 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.