



[Billing Code 7709-02-P]

PENSION BENEFIT GUARANTY CORPORATION

29 CFR Part 4902

Privacy Act Regulation; Exemption for Insider Threat Program Records

AGENCY: Pension Benefit Guaranty Corporation.

ACTION: Final rule.

SUMMARY: The Pension Benefit Guaranty Corporation (PBGC) is adopting as final an interim final rule to amend PBGC's Privacy Act regulation to exempt a system of records that supports a program of insider threat detection and data loss prevention.

DATES: This final rule is effective [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

FOR FURTHER INFORMATION CONTACT: Melissa Rifkin (rifkin.melissa@pbgc.gov), Attorney, Regulatory Affairs Division, Office of the General Counsel, Pension Benefit Guaranty Corporation, 1200 K Street NW, Washington, DC 20005-4026; 202-229-6563; Shawn Hartley (hartley.shawn@pbgc.gov), Chief Privacy Officer, Office of the General Counsel, 202-229-6435. TTY users may call the Federal relay service toll-free at 800-877-8339 and ask to be connected to 202-229-6435.

SUPPLEMENTARY INFORMATION:

Executive Summary

On July 9, 2019, PBGC published an interim final rule to amend PBGC's regulation on Disclosure and Amendment of Records Pertaining to Individuals under the Privacy Act (29 CFR part 4902) to exempt from disclosure information contained in a new system of records for

PBGC's insider threat program.¹ The exemption was needed because records in this new system include investigatory material compiled for law enforcement purposes. PBGC is adopting the interim final rule as final with minor, technical amendments.

Authority for this rule is provided by section 4002(b)(3) of the Employee Retirement Income Security Act of 1974 (ERISA) and 5 U.S.C. 552a(k)(2).

Background

The Pension Benefit Guaranty Corporation (PBGC) administers the pension plan insurance programs under title IV of the Employee Retirement Income Security Act of 1974 (ERISA). As a Federal agency, PBGC is subject to the Privacy Act of 1974, 5 U.S.C. 552a (Privacy Act), in its collection, maintenance, use, and dissemination of any personally identifiable information that it maintains in a "system of records." A system of records is defined under the Privacy Act as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."²

On July 9, 2019, PBGC established a new system of records, "PBGC-26, PBGC Insider Threat and Data Loss Prevention – PBGC"³

Executive Order 13587, issued October 7, 2011, requires Federal agencies to establish an insider threat detection and prevention program to ensure the security of classified networks and the responsible sharing and safeguarding of classified information consistent with appropriate protections for privacy and civil liberties. While PBGC does not have any classified networks, it does maintain a significant amount of Controlled Unclassified Information (CUI)

¹ 84 FR 32618 (July 9, 2019).

² See 5 U.S.C. 552a(a)(5).

³ 84 FR 32786 (July 9, 2019).

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. This system collects and maintains Personally Identifiable Information (PII) in the course of scanning traffic leaving PBGC's network and blocking traffic that violates PBGC's policies to safeguard PII.

This system covers "PBGC insiders," who are individuals with access to PBGC resources, including facilities, information, equipment, networks, and systems. This includes Federal employees and contractors. Records from this system will be used on a need-to-know basis to manage insider threat matters; facilitate insider threat investigations and activities; identify threats to PBGC resources, including threats to PBGC's personnel, facilities, and information assets; track tips and referrals of potential insider threats to internal and external partners; meet other insider threat program requirements; and investigate/manage the unauthorized or attempted unauthorized disclosure of PII.

Exemption

Under section 552a(k) of the Privacy Act, PBGC may promulgate regulations exempting information contained in certain systems of records from specified sections of the Privacy Act including the section mandating disclosure of information to an individual who has requested it. Among other systems, PBGC may exempt a system that is "investigatory material compiled for law enforcement purposes."⁴ Under this provision, PBGC has exempted, in § 4209.11 of its Privacy Act regulation, records of the investigations conducted by its Inspector General and contained in a system of records entitled "PBGC-17, Office of Inspector General Investigative File System—PBGC."

⁴ See 5 U.S.C. 552a(k)(2).

The PBGC-26, PBGC Insider Threat and Data Loss Prevention – PBGC system contains: 1) records derived from PBGC security investigations, 2) summaries or reports containing information about potential insider threats or the data loss prevention program, 3) information related to investigative or analytical efforts by PBGC insider threat program personnel, 4) reports about potential insider threats obtained through the management and operation of the PBGC insider threat program, and 5) reports about potential insider threats obtained from other Federal Government sources. The records contained in this new system include investigative material of actual, potential, or alleged criminal, civil, or administrative violations and law enforcement actions. These records are within the material permitted to be exempted under section 552a(k)(2) of the Privacy Act.

On July 9, 2019, at, PBGC published an interim rule adding a new § 4902.12 to its Privacy Act regulation.⁵ This addition exempts PBGC-26, PBGC Insider Threat and Data Loss Prevention – PBGC, from 5 U.S.C. 552a(c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f). Exemption from these sections of the Privacy Act means that, with respect to records in the system, PBGC is not required to: 1) disclose records to an individual upon request, 2) keep an accounting of individuals who request records, 3) maintain only records as necessary to accomplish an agency purpose, or 4) publish notice of certain revisions of the system of records.

PBGC provided the public 30 days in which to comment on the amendment made by the interim final rule and received comments from one commenter. PBGC considered the comments but is not modifying the regulation.

The commenter suggested that any data which is subject to breach or hacking should be made available to affected individuals and other interested persons, including the journalism

⁵ 84 FR 32618 (July 9, 2019).

community. Under 5 U.S.C. 552a(b), an agency is prohibited from disclosing any record contained in a system of records to any person unless it has obtained written consent from the subject of the record or the disclosure falls within one of the twelve exceptions articulated in that section. There is no exception that would permit PBGC to provide data that is subject to a “breach or hacking” to interested persons. Providing this information would be a violation of the Privacy Act.

The commenter suggested that the use of collected data must be strictly limited to necessary purposes, and broad collection of personal data, for investigations of insider threats, without access for review or correction of improper or unnecessary data should not be permitted. PBGC only collects the information it is authorized to collect and uses it for the purposes identified in its system of records notices. PBGC has listed the sources of records it anticipates collecting; however, to the extent that listing a source would potentially compromise a source of law enforcement information, PBGC has exempted this system of records under 5 U.S.C. 552a(e)(4)(I). Moreover, PBGC has exempted records maintained in this system of records from access to and amendment of records because providing access and amendment rights to such records could compromise or lead to the compromise of information that could warrant an invasion of another’s privacy, reveal a sensitive investigative technique, potentially allow a suspect avoid detection or apprehension, or constitute potential danger to a confidential source or witness.

Finally, the commenter stated that an objective third party should be an option for review of data if requested by an affected individual or group, subject to reasonable confidentiality protections necessary to protect any legitimate law enforcement or investigatory purposes. Any disclosure of insider threat information, including disclosure to an “objective third party,” could

substantially compromise an investigation of insider threat activities. For example, that information may identify the subject of the investigation or a witness who was promised confidentiality. PBGC does not know who the “objective third party” is or with whom the information might be shared. Further, there are no “reasonable confidentiality protections” that would prevent that information from getting into the wrong hands. Moreover, if the “affected individual or group” means those persons who were subjected to an unauthorized or attempted unauthorized disclosure of PII, providing that information to an “objective third party” may invade the privacy of “the affected individual or group.” Finally, disclosure may also compromise the investigation by revealing law enforcement techniques and procedures.

Accordingly, PBGC adopts the interim final rule as final with minor, technical amendments to remove the introductory text in § 4902.12(a) and redesignate the paragraphs.

Compliance with Rulemaking Guidelines

The interim final rule was exempt from the requirements of prior notice and comment and a 30-day delay in effective date because it is a rule of “agency organization, procedure, or practice” and is limited to “agency organization, management, or personnel matters.” *See* 5 U.S.C. 553(a), (b), (d). The exemption from provisions of the Privacy Act provided by the interim final rule affects only PBGC insiders described above. Nonetheless, PBGC provided an opportunity for post-promulgation comment. As this rule is the finalization of an interim final rule and is a rule of agency organization, procedure, or practice, further request for comment and a 30-day delay in effective date are not required. Because this rule is exempt from notice and public comment requirements under 5 U.S.C. 553(b), it is also exempt from the requirements of

Executive Order 12866 and Executive Order 13771,⁶ and the Regulatory Flexibility Act does not apply to this rule. *See* 5 U.S.C. 601(2), 603, 604.

List of Subjects in 29 CFR Part 4902

Privacy

In consideration of the foregoing, the interim rule amending 29 CFR part 4902 which was published at 84 FR 32618 on July 9, 2019, is adopted as final with the following change:

PART 4902—DISCLOSURE AND AMENDMENT OF RECORDS PERTAINING TO INDIVIDUALS UNDER THE PRIVACY ACT

- 1. The authority citation will continue to read as follows:

Authority: 5 U.S.C. 552a, 29 U.S.C. 1302(b)(3).

§ 4902.12 [Amended]

- 2. In § 4902.12:
 - a. Remove the paragraph (a) subject heading; and
 - b. Redesignate paragraphs (a)(1) and (2) as paragraphs (a) and (b), respectively.

Issued in Washington, DC.

Gordon Hartogenesis,

Director,

Pension Benefit Guaranty Corporation

[FR Doc. 2020-19950 Filed: 10/7/2020 8:45 am; Publication Date: 10/8/2020]

⁶ *See* section 3(d)(3) of Executive Order 12866 and section 4(b) of Executive Order 13771.