

2020–20–17 General Electric Company:
Amendment 39–21273; Docket No.
FAA–2020–0902; Project Identifier AD–
2020–01174–E.

(a) Effective Date

This AD is effective October 23, 2020.

(b) Affected ADs

None.

(c) Applicability

This AD applies to all General Electric Company GE90–110B1 and GE90–115B model turbofan engines.

(d) Subject

Joint Aircraft System Component (JASC)
Code 7600, Engine Controls.

(e) Unsafe Condition

This AD was prompted by an in-service occurrence of loss of engine thrust control resulting in uncommanded high thrust. The FAA is issuing this AD to prevent dispatch of the airplane when certain faults caused by degradation of the MN4 integrated circuit in the full authority digital engine control (FADEC) are displayed and certain FADEC conditions are present. The unsafe condition, if not addressed, could result in loss of engine thrust control and reduced control of the airplane.

(f) Compliance

Comply with this AD within the compliance times specified, unless already done.

(g) Required Actions

After the effective date of this AD, notwithstanding the provisions of the operator's minimum equipment list (MEL), dispatch of an airplane is prohibited if the engine indicating and crew alerting system (EICAS) displays the status message "ENG EEC C1 L" or "ENG EEC C1 R" and any condition is present that is listed in the Accomplishment Instructions, paragraphs 3.A.(2)(f), 3.A.3(a), or 3.A.(4) of GE GE90–100 Service Bulletin (SB) 73–0117 R01, dated August 5, 2020.

(h) Terminating Action

As terminating action for the requirements of paragraph (g) of this AD, within 120 days of the effective date of this AD, revise the existing FAA-approved MEL by incorporating into the MEL the dispatch restrictions listed in paragraph (g) of this AD as a required operation or maintenance procedure. Specific alternative MEL wording to accomplish the actions specified in paragraph (g) of this AD can be approved by the operator's principal operations or maintenance inspector.

(i) Alternative Methods of Compliance (AMOCs)

(1) The Manager, ECO Branch, FAA, has the authority to approve AMOCs for this AD, if requested using the procedures found in 14 CFR 39.19. In accordance with 14 CFR 39.19, send your request to your principal inspector or local Flight Standards District Office, as appropriate. If sending information directly to the manager of the certification office,

send it to the attention of the person identified in paragraph (j) of this AD. You may email your request to: ANE-AD-AMOC@faa.gov.

(2) Before using any approved AMOC, notify your appropriate principal inspector, or lacking a principal inspector, the manager of the local flight standards district office/certificate holding district office.

(j) Related Information

For more information about this AD, contact Stephen Elwin, Aerospace Engineer, ECO Branch, FAA, 1200 District Avenue, Burlington, MA 01803; phone: 781–238–7236; fax: 781–238–7199; email: stephen.l.elwin@faa.gov.

(k) Material Incorporated by Reference

(1) The Director of the Federal Register approved the incorporation by reference (IBR) of the service information listed in this paragraph under 5 U.S.C. 552(a) and 1 CFR part 51.

(2) You must use this service information as applicable to do the actions required by this AD, unless the AD specifies otherwise.

(i) General Electric Company (GE) GE90–100 Service Bulletin 73–0117 R01, dated August 5, 2020.

(ii) [Reserved]

(3) For GE service information identified in this AD, contact General Electric Company, 1 Neumann Way, Cincinnati, OH 45215; phone: 513–552–3272; email: aviation.fleetsupport@ge.com; website: www.ge.com.

(4) You may view this service information at FAA, Airworthiness Products Section, Operational Safety Branch, 1200 District Avenue, Burlington, MA 01803. For information on the availability of this material at the FAA, call 781–238–7759.

(5) You may view this service information that is incorporated by reference at the National Archives and Records Administration (NARA). For information on the availability of this material at NARA, email: fedreg.legal@nara.gov, or go to: <https://www.archives.gov/federal-register/cfr/ibr-locations.html>.

Issued on September 25, 2020.

Lance T. Gant,

*Director, Compliance & Airworthiness
Division, Aircraft Certification Service.*

[FR Doc. 2020–22267 Filed 10–7–20; 8:45 am]

BILLING CODE 4910–13–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 October 8, 2020.

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,

¹ 84 FR 32618 (July 9, 2019).

² See 5 U.S.C. 552a(a)(5).

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) 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.”

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 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

³ 84 FR 32786 (July 9, 2019).

⁴ See 5 U.S.C. 552a(k)(2).

⁵ 84 FR 32618 (July 9, 2019).

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 Hartogensis,
Director, Pension Benefit Guaranty Corporation.

[FR Doc. 2020–19950 Filed 10–7–20; 8:45 am]

BILLING CODE 7709–02–P

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

DEPARTMENT OF HOMELAND SECURITY

Coast Guard

33 CFR Part 165

[Docket No. USCG–2020–0579]

Safety Zone, Brandon Road Lock and Dam to Lake Michigan Including Des Plaines River, Chicago Sanitary and Ship Canal, Chicago River, and Calumet-Saganashkee Channel, Chicago, IL

AGENCY: Coast Guard, DHS.

ACTION: Notice of enforcement of regulation.

SUMMARY: The Coast Guard will enforce a segment of the Safety Zone; Brandon Road Lock and Dam to Lake Michigan including Des Plaines River, Chicago Sanitary and Ship Canal, Chicago River, Calumet-Saganashkee Channel on all waters of the Chicago Sanitary and Ship Canal and South Branch of the Chicago River between mile marker 296 and mile marker 296.7 during specified times from September 25, 2020 through October 29, 2020. This action is necessary and intended to protect the safety of life and property on navigable waters prior to, during, and immediately after planned US Army Corps of Engineers work at the Electric Barrier. During the enforcement period listed below, entry into, transiting, or anchoring within the safety zone is prohibited unless authorized by the Captain of the Port Lake Michigan or a designated representative.

DATES: The regulations in 33 CFR 165.930 will be enforced from 7 a.m. through 11 a.m. and 1 p.m. through 5 p.m. daily without actual notice from October 8, 2020 through 5 p.m. on October 29, 2020. For purposes of enforcement, actual notice will be used 7 a.m. through 11 a.m. and 1 p.m. through 5 p.m. daily from September 25, 2020 through October 8, 2020.

FOR FURTHER INFORMATION CONTACT: If you have questions about this notice of enforcement, call or email LT Tiziana Garner, Waterways Management Division, Marine Safety Unit Chicago, at 630–986–2155, email address *D09-DG-MSUChicago-Waterways@uscg.mil*.

SUPPLEMENTARY INFORMATION: The Coast Guard will enforce a segment of the Safety Zone; Brandon Road Lock and Dam to Lake Michigan including Des Plaines River, Chicago Sanitary and Ship Canal, Chicago River, Calumet-Saganashkee Channel on all waters of the Chicago Sanitary and Ship Canal and South Branch of the Chicago River

between mile marker 296 and mile marker 296.7 during specified times from September 25, 2020 through October 29, 2020. This action is necessary and intended to protect the safety of life and property on navigable waters prior to, during, and immediately after planned US Army Corps of Engineers work at the Electric Barrier. During the enforcement period, entry into, transiting, or anchoring within the safety zone is prohibited unless authorized by the Captain of the Port Lake Michigan or a designated representative.

This notice of enforcement is issued under the authority of 33 CFR 165.930 and 5 U.S.C. 552(a). In addition to this notice of enforcement in the **Federal Register**, the Coast Guard will provide notification of this enforcement period via Broadcast Notice to Mariners, Local Notice to Mariners, distribution in leaflet form, and on-scene oral notice. Additionally, the Captain of the Port Lake Michigan may notify representatives of the maritime industry through telephonic and email notifications. If the Captain of the Port or a designated representative determines that the regulated area need not be enforced for the full duration stated in this notice, he or she may use a Broadcast Notice to Mariners to grant general permission to enter the regulated area. The Captain of the Port Lake Michigan or a designated on-scene representative may be contacted via Channel 16 or at (414) 747–7182.

Dated: September 16, 2020.

Donald P. Montoro,
Captain, U.S. Coast Guard, Captain of the Port, Lake Michigan.

[FR Doc. 2020–20790 Filed 10–7–20; 8:45 am]

BILLING CODE 9110–04–P

ENVIRONMENTAL PROTECTION AGENCY

40 CFR Part 62

[EPA–R10–OAR–2020–0074; FRL–10011–40–Region 10]

Approval and Promulgation of State Plans for Designated Facilities and Pollutants; Oregon Department of Environmental Quality; Control of Emissions From Existing Municipal Solid Waste Landfills

AGENCY: Environmental Protection Agency (EPA).

ACTION: Final rule.

SUMMARY: The Environmental Protection Agency (EPA) is taking final action to approve a state plan submitted by the