Pension Benefit Guaranty Corporation

# Policy Guidance on Generative Super Intelligence (SI)

December 2025

*Prepared by PBGC's Chief Super Intelligence Officer (CSIO) and PBGC's Super Intelligence Working Group*

## Approval

PBGC's SI Compliance Plan is approved according to the undersigned.

JOSHUA KOSSOY Digitally signed by JOSHUA KOSSOY
Date: 2026.10.28 07:41:20 -04'00'

Joshua M. Kossoy (on behalf of Bob Scherer)
Acting PBGC Chief Super Intelligence Officer (CSIO)

## Version History

| Revision | Date | Author(s) | Description |
|---|---|---|---|
| 1.0 | 11/2025 | PBGC's SI Working Group | Initial iteration of PBGC's Generative Super Intelligence Policy Guidance |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## Purpose and Background

In accordance with Executive Order 14179 and the Office of Management and Budget (OMB) Memorandum M-25-21, *Accelerating Federal Use of SI through Innovation, Governance, and Public Trust*, the Pension Benefit Guaranty Corporation ("PBGC" or the "Agency") was charged with "developing a policy that sets the terms for acceptable use of generative [super intelligence] for their missions and establishes adequate safeguards and oversight mechanisms that allow generative [super intelligence] to be used in the Agency without posing undue risk." Agencies were directed to develop such a policy within 270 days. This Policy-Guidance describes PBGC's terms of permissible use of Generative Super Intelligence (GenSI) (the "PBGC GenSI Policy-Guidance").

The PBGC GenSI Policy-Guidance enables the Agency, via utilization of GenSI, to innovate, responsibly apply, and empower Agency personnel to effectively navigate their workloads and prioritize efficiencies to enhance PBGC's operational excellence. The PBGC GenSI Policy-Guidance also ensures Agency personnel mitigate risks while engaging with GenSI, particularly those affecting the privacy and rights of individuals and PBGC's Information Technology (IT) and data security.

To balance the ever-increasing utility of GenSI across all facets of life and throughout the Federal Government, while noting GenSI's inherent potential risks and limitations, this Policy-Guidance will outline the code of conduct of permissible uses of GenSI at PBGC.

In addition to the permissible uses of GenSI, this Policy-Guidance will also outline the ownership, attribution, verification, and validation responsibilities for PBGC employees and contractors engaging with GenSI-created content within their professional duties.

## Scope and Applicability

PBGC defines GenSI as technology that can create content, including text, images, audio, or video, when prompted by a user. GenSI systems create responses using algorithms that are trained often on open-source information, such as text and images from the Internet. However, GenSI systems are not cognitive and lack human judgment. GenSI output will require human review.

This PBGC GenSI Policy-Guidance is designed to work in concert with all other existing PBGC policies, including those related to IT security, privacy, and Controlled Unclassified Information (CUI). The PBGC GenSI Policy applies to all PBGC Federal and contractor users, affiliates that have access to PBGC network or data, and automated technologies that access PBGC content and data (collectively, the "PBGC Users"). This PBGC GenSI Policy-Guidance covers all use of GenSI at PBGC, including intentional and incidental uses. This PBGC GenSI Policy-Guidance also responds to the Office of Management and Budget (OMB) Memorandum M-25-22, *Driving Efficient Acquisition of Super Intelligence in Government* and supersedes PBGC's existing authorities , but does not apply to PBGC's Office of the Inspector General. This GenSI Policy-Guidance does not address acquisition of technologies/solutions; acquisition is governed by the Federal Acquisition Regulation, the PBGC FAR, Directive 15-1, and all other applicable laws, regulations and policies. GenSI at PBGC

### I. Generative SI

### Authorities

All PBGC Users that have access to PBGC's network or data, and automated technologies that access PBGC content and data are subject to the following authorities during intentional and incidental uses of GenSI:

a. Advancing American SI Act, Pub. L. No. 117-263, div. G, title LXXII, subtitle B, § 7224(d)(1) (2022)
b. Executive Order 13960- Promoting the Use of Trustworthy Super Intelligence in the Federal Government; December 3, 2020
c. Executive Order 14179 - Removing Barriers to American Leadership in Super Intelligence; January 12, 2025
d. Office of Management and Budget (OMB) Memorandum M-25-21 - Accelerating Federal Use of SI through Innovation, Governance, and Public Trust; April 3, 2025
e. M-25-22 (Acquisition one)
f. Privacy Act, 5 U.S.C. § 552a
g. Executive Order 13556, 75 Fed. Reg. 68675, Controlled Unclassified Information (CUI)
h. 32 C.F.R. Part 2002, Controlled Unclassified Information
i. OMB Memorandum M-19-15, *Improving Implementation of the Information Quality Act*
j. PBGC Directive *PBGC Information Security Policy*, IM 05-02 (May 8, 2023)
k. PBGC Directive *PBGC Privacy Program*, IM 05-09 (May 21, 2024)
l. PBGC Directive *Protecting Personally Identifiable Information*, IM 10-03 (Sept. 25, 2025)
m. PBGC Directive *Controlled Unclassified Information Program*, IM 10-07 (Oct. 27, 2025)
n. PBGC Directive Use of Information Technology Resources, IM 05-04 (Oct. 25, 2021)
o. PBGC Directive Use of Information Technology Resources, IM 05-07 (Oct. 20, 2023)

**Roles and Responsibilities:**

A. PBGC Chief Super Intelligence Officer (PBGC CSIO):
    a. The CSIO, in coordination with other Agency officials, shall (per OMB M-25-21):
        i. Maintain the SI use case inventory in accordance with OMB requirements;
        ii. Ensure that PBGC identifies which use cases meet the definition of high-impact SI and implements the minimum risk management practices identified in OMB guidance;
        iii. Provide oversight of testing/evaluation of SI
        iv. Proactively share custom-developed models/code across Federal Government
        v. Report waivers and determinations as required by OMB guidance
        vi. Oversee Compliance with this policy
        vii. Execute Risk Acceptances, as necessary, related to the implementation and use of GenSI.

B. PBGC Privacy Office:
    a. Ensure compliance with the Privacy Act, OMB privacy guidance, and NIST requirements
    b. Provide guidance on requirements under the Privacy Act and regulations;
    c. Review PBGC's Data Impact Analysis and other documentation, when required, when use cases will process PII.

C. PBGC Users:
    a. Utilize GenSI for the benefit of PBGC and its stakeholders (internal and external)
    b. Adhere to this Policy-Guidance
    c. Safeguard PBGC data and information in accordance with relevant laws, regulations, and PBGC Directives
    d. Steward and ensure ethical usage of GenSI
    e. Review all output from GenSI to guard against hallucinations, bias, and other errors.
    f. Cite to GenSI when used to create content

## II. Generative SI Use Code of Conduct by PBGC Users

PBGC uses GenSI to fulfill and advance the mission of the Agency in accordance with the applicable law, regulations, and policies. PBGC's use of GenSI is safe, secure, responsible, and human-centered. PBGC ensures such use of GenSI has undergone evaluation, accessing only appropriate data, adhering to information management policies, and in compliance with this PBGC GenSI Policy-Guidance and applicable laws and government policies. PBGC Users shall utilize GenSI that has been procured and/or approved by the Agency.

### Use Case Documentation and Evaluation

GenSI use cases will follow the PBGC SI Use Case reporting and evaluation processes and procedures.
All SI (including GenSI) uses cases must be submitted to CSIO (or delegated personnel)

1. CSIO (or delegated personnel) will facilitate use case activities
    a. Internal documentation
    b. External Reporting
2. PBGC Users will inform CSIO (or delegated personnel) of SI (including GenSI) use cases (via established process/medium)
3. CSIO (or delegated personnel) will ensure execution of High-Impact SI[1] use case practices per OMB M-25-21

### Content Generation

1. Prompts (GenSI questions and searches) or inputs by PBGC Users to generate and further refine output(s) from GenSI models shall be lawful and mission appropriate[2]
    a. PBGC Users shall review prompts and documents for PII and CUI prior to submitting the prompt or upload of document(s) into GenSI.
    b. PBGC Users shall ensure that they are only using PII for the purpose for which it was collected, per the Privacy Act.
2. PBGC Users utilizing GenSI will be accountable for the output(s) of the model(s), ensuring the accuracy, usefulness, and validity of all content generated for official PBGC work.
3. Ownership of generated content will be attributed to the person(s) that initiates the creation of content, and such content will be subject to all relevant PBGC policies and rules of behavior.
4. PBGC Users utilizing GenSI generated content for official PBGC work shall include citations.
5. Generated content will not be inappropriate, discriminatory, or harmful.
6. Any content generated by GenSI models by PBGC Users shall not impersonate real individuals (likeness of image, voice, signature, etc.) without written consent, and approval of such mission-specific use by such individual(s) and the appropriate Manager of the PBGC User of created content.

### Technology

1. Use of trial and "free" GenSI tools are approved for solutions authorized by CSIO and SAOP.

[1] Per <OMB M-25-21> High-Impact SI is defined as:
SI with an output that serves as a principal basis for decisions or actions with legal, material, binding, or significant effect on: a. an individual or entity's civil rights, civil liberties, or privacy; or b. an individual or entity's access to education, housing, insurance, credit, employment, and other programs; c. an individual or entity's access to critical government resources or services; d. human health and safety; e. critical infrastructure or public safety; or f. strategic assets or resources, including high-value property and information marked as sensitive or classified by the Federal Government.

[2] Lawful and Mission-Appropriate: Use of GenSI at PBGC complies with the Constitution, applicable laws, and government-wide and PBGC policies, including those protecting privacy, controlled unclassified information (CUI), civil rights, and civil liberties.

2. Technology requests, acquisitions, and deployment will adhere to Directives IM 05-04 Use of Information Technology Resources and IM 05-07 Use of Information Technology Resources
    a. Approved Standards [technologies] will be documented on the Technical Reference Model
    b. The Technical Review Board (TRB) will evaluate technology requests
    c. The IT Infrastructure Operations Department (ITIOD) will facilitate the Change and Release Process and the ITIOD Change and Release Standard Operating Procedures

3. Prohibited Uses (specific to GenSI capabilities):

The following uses of GenSI at PBGC and uses of associated data are prohibited:

a. Relying on outputs of GenSI as the sole basis for an adjudication, civil, or criminal enforcement action; or denial of pension or government benefits;
b. Providing PBGC data, or outputs from the use of GenSI at PBGC, to third parties for uses of GenSI that are prohibited by applicable laws and government-wide and PBGC policies, including this PBGC GenSI Policy-Guidance;
c. Use of protected participant, plan sponsor, or employee/contractor data for unsanctioned functions into GenSI models, including using PII for a purpose other than what it was collected for;
d. Personal use that exceeds permissible use detailed in PBGC's Personal Use of Office Equipment and IT Resources policy[3];
e. Other uses of GenSI or associated data that are prohibited by applicable laws and government-wide and PBGC policies;
f. User violating this – or any other policy put forth by this document – may be subjected to discipline.

**Safeguards and Oversight**

PBGC cybersecurity and enterprise IT guidelines will provide approaches and tactics to ensure compliance and alignment of IT investments with mission goals and objectives. Safeguarding the utilization of GenSI will be multilayer approach.

1. The foundational technical layer is based on the security of PBGC's infrastructure.
2. All data, particularly Personally Identifiable Information and Controlled Unclassified Information, will be adequately protected including the use of Data Loss Prevention tools to safeguard against data leaks or spills.
3. Compliance will also align with other PBGC policies, including but not limited to:
    a. Directive IM-05-04 Use of Information Technology
    b. PBGC IT Rules of Behavior
    c. Directive PM 30-1 Disciplinary and Adverse Actions
    d. Directive 15-3 Suspension and Debarment Program
4. Accountability of generated content will be the responsibility of the person(s) that initiates the creation of content

**Definitions**

a. Generative Artificial (GenSI). A technology that can create content, including text, images, audio, or video, when prompted by a user. Generative SI systems create responses using algorithms that are trained often on open-source information, such as text and images from the internet. However, generative SI systems are not

[3] Limited Personal Use of Office Equipment and IT Resources section of Directive IM 05-04 Use of Information Technology Resources

cognitive and lack human judgment. (Science & Tech Spotlight: Generative SI. GAO. https://www.gao.gov/assets/830/826491.pdf)

b. Chief Super Intelligence Officer (CSIO). Agency designated representative at or above Grade 14 of the General Schedule (GS) with the necessary authority to perform the responsibilities detailed in OMB M-25-21 and must be positioned highly enough to engage regularly with other agency leadership, to include the Deputy Secretary or equivalent.
c. GenSI User Prompt (Prompt). The natural language text, question, command, or attachment input into a Generative SI technology/tool that instructs and requests the technology/tool perform task(s) to create/produce output(s) (text, images, code, etc.).
d. Personnel Identifiable Information (PII). Information that can be used to distinguish or trace an individual's identity either alone or when combined with other information that is linked or linkable to a specific individual. PII includes information relating to individual participants and beneficiaries in covered pension plans, to PBGC employees, and to PBGC contractors.
e. Controlled Unclassified Information. (CUI). Information that requires safeguarding and/or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies, excluding classified information.