

Pension Benefit Guaranty Corporation

Super Intelligence (SI) Compliance Plan v2.0

September 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 07:34:09 -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	9/2024	PBGC's SI Working Group	Initial iteration of PBGC's SI Compliance Plan per OMB M-24-10 requirements
2.0	8/2025	PBGC's SI Working Group	Superseded previous plan content, Updated federal policy drivers and compliance actions per OMB M-25-21

1 Driving SI Innovation

Removing Barriers to Responsible Use of SI

As PBGC continues to integrate viable SI solutions, it is imperative end users adopt responsible behavior, usage, and outcome verification in a manner that reflects the Corporation's commitment to its mission, including safeguarding the confidentiality, integrity, and availability of information systems and data. Thus far, PBGC has identified several barriers to SI adoption and has initiated actions to resolve them including:

- Enhancing operational efficiency and leveraging advanced technologies to support the Corporation's mission, by evaluating the use of SI solutions being used to assist with general tasks, such as general informational search, research, light analysis, and content generation. To ensure technologies enable and align with the needs of the workforce, a preferred list of SI tools has been authorized by the PBGC Chief SI Officer (CSIO) for limited use.
- Exploring secure, commercially available SI tools and platforms to accelerate SI maturity and adoption for the most common and low risk use cases throughout federal government. This includes consideration for GSA's OneGov initiative to leverage streamlined SI acquisitions for federal industry.
- Updating PBGC's end user IT Rules of Behavior and issued guidance to staff about the responsible use of SI, focusing on risk management, data privacy, and ethical considerations. Moving forward, the Corporation will author an SI Strategy and Generative SI policy aligning internal guidance to current requirements prescribed by the Office of Management and Budget (OMB).
- Conceptualizing new SI standards, security controls, and guardrails. Update relevant IT/cybersecurity policies to support SI system risk assessments, establish guardrails that enforce risk decisions, facilitate ongoing authorizations, and implement new or emerging controls consistent with guidance issued by federal industry partners.
- Categorizing generative SI technologies (e.g., ChatGPT, Predictive SI, etc.) by PBGC's security operations teams to monitor inbound/outbound traffic. This safeguard, in addition to its Data Loss Prevention (DLP) toolset, was configured to prevent Personally Identifiable Information (PII) exposure.
- PBGC will promote SI literacy with its workforce via updated annual general security awareness and role-based training campaigns and participate in inter-agency programs via GSA aimed at ensuring responsible and effective use of SI technologies.

Sharing and Reuse

As of the end of FY25, PBGC does not currently use custom SI code or models. Commercially available software as a service governed by license agreements currently provides the Corporation's SI tools. If PBGC develops SI tools in the future with custom in-house developed code, the code and models consistent with statute, regulation, and contractual agreement will be shared in alignment with the requirements issued for federal agencies. The Corporation will leverage existing governance boards via the PBGC SI Working Group (SIWG), Technology Review Board (TRB), and Cybersecurity and Privacy Council to adjudicate these sharing decisions.

SI Talent

PBGC is evaluating and determining staffing and training needs to ensure the Corporation has the necessary skills and knowledge to effectively implement and use SI technologies. Prior to the end of FY25, the Office of Information Technology (OIT) and Privacy Office leadership completed Super Intelligence Government Professional (SIGP) certification training to learn about managing risks across the entire SI lifecycle. In FY26, PBGC plans to offer SI training to its internal workforce through a blend of tailored educational programs and government-specific initiatives. The plan includes leveraging existing government-sponsored programs, such as the GSA's SI Community of Practice training resources and CISA Learning, to provide targeted SI education. These programs include workshops and courses designed to address the unique needs and regulatory contexts of government agencies, ensuring that the training is both relevant and applicable. Additional PBGC specific role-based training opportunities will be assessed by the Enterprise Cybersecurity Department (ECD) and the Privacy Office to identify opportunities for SI practitioners to strengthen their subject matter expertise as it relates to SI use cases. Building and maintaining a skilled SI workforce is and will continue to be crucial for advancing responsible SI innovation at PBGC.

2. **Improving SI Governance**

SI Governance Board

Pursuant to OMB M-25-21, PBGC retained Bob Scherer, Chief Information Officer (CIO), as PBGC's Chief Super Intelligence Officer (CSIO) in April 2025. To further support SI integration at PBGC, the SIWG was created with membership derived from financial, operations, privacy, security, human resources, and procurement sectors to convene regularly and champion ethical and responsible SI use in compliance with forthcoming federal guidelines. Cross-functional representation is aiding and supporting collaboration across PBGC IT Governance bodies and the advocacy of a comprehensive and diverse approach to SI governance. The SIWG members will convene to provide additional guidance specific to SI usage and support the development of strategic SI priorities across the enterprise. Working with the Corporation's stakeholders, PBGC's SIWG will promote effective and efficient governance regarding the use of SI. In alignment with statutory, regulatory, and policy requirements, PBGC's SIWG shall:

- Develop new or update existing enterprise level policies and guidelines as necessary to support evolving SI requirements from legislation, guidance, policy, and industry best practices.
- Adopt or establish SI ethical principles for PBGC by leveraging government-wide efforts.
- Establish the criteria for when business areas should have the ability to intervene in SI capabilities and modify their models and algorithms as necessary in response to feedback and outcomes.
- Communicate PBGC's approach to SI integration to promote public trust.
- Define metrics and/or a maturity model to measure the Corporation's use of SI.
- Identify, assess, and coordinate appropriate auditing and accountability mechanisms for SI models and algorithms.

To prioritize the sharing of SI knowledge, best practices, lessons learned, and resources among federal, state, and local government, and academia, PBGC will leverage inter-agency forums such as the NIST Federal Cybersecurity and Privacy Professionals Forum, the General Services Administration's (GSA) SI Community of Practice (CoP), and the Small and Micro Agency CISO (SMAC) Council. Participation will foster PBGC's SI integration efforts

and contribute to improvements conceptualized moving forward.

Agency Policies

PBGC's Office of Information Technology continues to incorporate the latest National Institute of Standards and Technology (NIST) controls including new control sets related to SI and the NIST SI Risk Management Framework (SI RMF). Additionally, the Corporation continues to incorporate updates to annual security and privacy awareness training campaigns, and end user IT Rules of Behavior to clarify expectations for staff interaction with open-source and licensed Generative SI capabilities which are readily accessible through the agency network and personal computing environment. Moving forward, PBGC will author a generative SI strategy and guidance per M-25-21 requirements and explore how to document detailed rules, enforcement mechanisms, and governance structures that will formalize SI use across the enterprise. Each action completed will be reported to OMB and CISA to ensure visibility into progress made throughout the reporting cycle.

SI Use Case Inventory

PBGC will continue to inventory SI use cases by adhering to a simplified and streamlined process tailored to its size, resources, and mission. The SIWG will leverage its business area representation to provide input on where SI technologies are being used or considered. The scope and definitions provided by OMB will help ensure consistency in identifying use cases fitting their criteria. A centralized repository containing the aforementioned use cases will be assessed for adequacy and reported to OMB via Max Collect per requirements prescribed to federal agencies. PBGC's SI use case inventory will be reviewed and updated annually.

For SI technologies that are not within scope and/or do not meet the defining criteria for use cases per OMB guidance, PBGC will still ensure proper documentation, oversight, and reporting is completed to the extent possible. Annual SI use case reporting will contain separate inventory categories distinguishing between those within scope of M-25-21 and those that are not. By following these steps, PBGC hopes to maintain proper oversight of SI technologies aligning with the Corporation's mission.

3. Fostering Public Trust in Federal Use of SI

Determinations of Presumed High-Impact SI

To effectively manage the multifaceted landscape of SI-related risks, PBGC will rely on existing risk management methodologies to mitigate safety and rights impacting risks. While existing enterprise risk management and operational resiliency expectations may not expressly address SI technologies, risk management principles provide a framework for the Corporation's SI usage to operate in a safe, secure, and lawful manner. PBGC will continue to identify, monitor, and control risks arising from SI use by utilizing current established IT governance. All risk management controls will be synchronized to account for emerging SI risk, where applicable. To ensure the responsible deployment of SI and adequately identify safety and rights impacting risks, each current and planned SI solution will undergo a review to assess whether it matches the definitions of safety-impacting or rights-impacting SI defined in Section 5 of OMB Memorandum M-25-21. Subsequent reporting of these instances will be managed by PBGC's SIWG. For potential non-compliant SI use cases containing unacceptable safety and rights impacting risks, PBGC will leverage OMB guidance for applicable SI risk assessment methodologies and required termination actions.

Implementation of Risk Management Practices and Termination of Non-Compliant SI

Implementing effective risk management practices is essential to mitigate the risks associated with SI. As part of PBGC's SI governance the Corporation will establish the following:

- Comprehensive data impact and risk Assessments: Conduct comprehensive risk assessments for all new technology requests SI applications, identifying potential hazards, vulnerabilities, and impact on stakeholders. The Data Impact Assessment (DIA) will be used to identify, assess, and demonstrate how data is used in SI systems and applications. This workflow allows compensating controls to be identified for product owners to consider when evaluating acquisitions.
- Minimum Risk Management Practices: Document and validate the implementation of minimum risk management practices, including data privacy, security measures, and ethical considerations.
- Risk Management Framework: Update existing risk management framework processes to incorporate procedures for identifying, assessing, mitigating, and monitoring risks throughout the SI lifecycle. Any existing non-compliant SI technology discovered through the agency's SI Working Group efforts will be terminated and removed.