OFFICE OF INSPECTOR GENERAL

AUDIT REPORT

PBGC's Software Self-Attestation Efforts Need Improvement

Report No. AUD-2025-10
August 6, 2025

PBGC's Software Self-Attestation Efforts Need Improvement

Report Number: AUD-2025-10
Date: August 6, 2025

Brief Sheet

Background and Objective

Executive Order (EO) 14028, *Improving the Nation's Cybersecurity*, focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments.

To implement the EO, the Office of Management and Budget (OMB) issued memorandum M-22-18, requiring federal agencies to use only software from producers who can attest to complying with the government-specified secure software development practices described in National Institute of Standards and Technology (NIST) guidance. OMB then issued memorandum M-23-16, *Update to Memorandum M-22-18,* which reinforced the requirements established in M-22-18, reaffirmed the importance of secure software development practices, extended the agencies' timelines to collect attestations from critical software producers and provided supplemental guidance to agencies on the use of a Plan of Action and Milestones (POA&M) when a software producer cannot provide the required attestation.

Our objective was to evaluate PBGC's efforts regarding the software self-attestation requirements. Our review focused on critical software.

Audit Results

Conclusion. Overall, we found PBGC made some efforts to meet the critical software self-attestation requirements. Specifically, PBGC established a process for the Critical Software Inventory and obtained and stored some attestations for critical software.

However, while PBGC inventoried critical software, the inventory did not contain all the data elements needed. Additionally, we also found instances where the Corporation did not adequately collect, review, and manage attestations; this led to PBGC utilizing critical software that may not meet minimum secure software development requirements.

Recommendations/Management Response

We made five recommendations related to improving PBGC's Critical Software Inventory and self-attestation process. The Corporation agreed with the recommendations and plans to complete all recommendations by July 31, 2026. PBGC agreed to update and maintain a complete Critical Software Inventory; create or update guidance; ensure all responsible staff receive appropriate training; update PBGC's process documentation when software producers cannot attest to adhering to the secure software development practices; and contact OMB for clarifying guidance for outstanding attestations.

August 6, 2025

MEMORANDUM

TO: Bob Scherer
Chief Information Officer

FROM: John Seger
Assistant Inspector General for Audits, Evaluations, and Inspections

SUBJECT: Issuance of Final Report: PBGC's Software Self-Attestation Efforts Need Improvement (Report No. AUD-2025-10)

We are pleased to provide you with the above-referenced final report. We appreciate the cooperation you and your staff extended to the OIG during this project. We thank you for your receptiveness to our recommendations and your commitment to reducing risk and improving the effectiveness and efficiency of PBGC programs and operations.

This report contains public information and will be posted in its entirety on our website and provided to the Board and Congress in accordance with the Inspector General Act.

cc: Alice Maroni, PBGC Acting Director
Karen Morris, General Counsel, Office of the General Counsel
Lisa Carter, Acting Chief Financial Officer/Director, Corporate Controls and Reviews Department
Damon McClure, Director, Procurement Department
Latreece Wade, Risk Management Officer
Department of Labor Board staff
Department of Treasury Board staff
Department of Commerce Board staff
House committee staff (Education and Workforce, Ways and Means, HOGR)
Senate committee staff (HELP, Finance, HSGAC)

Table of Contents

Background

Established by the Employee Retirement Income Security Act of 1974, the Pension Benefit Guaranty Corporation (PBGC or the Corporation) protects the retirement security of about 31 million American workers, retirees, and beneficiaries in both single-employer and multiemployer private-sector pension plans. In Fiscal Year 2024, PBGC paid over $5.8 billion in benefits to 912,000 participants. To support its mission, one of the three strategic goals articulated in PBGC's Strategic Plan is to "maintain high standards of stewardship and accountability."

Secure Software Development Practices

Executive Order 14028, *Improving the Nation's Cybersecurity*, focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. The Executive Order directed the National Institute of Standards and Technology (NIST) to issue guidance "identifying practices that enhance the security of the software supply chain." NIST published Special Publication 800-218, *Secure Software Development Framework*, which included a set of practices creating the foundation for developing secure software. The Executive Order further directed the Office of Management and Budget (OMB) to require agencies to comply with such guidelines.

OMB issued memorandum M-22-18, *Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices* to comply with Executive Order 14028. The memorandum requires federal agencies to use only software from producers who can attest to complying with the government-specified secure software development practices described in NIST guidance.

Following M-22-18, OMB issued memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain Through Secure Software Development Practices*. M-23-16 reinforced the requirements established in M-22-18, reaffirmed the importance of secure software development practices, and extended the agencies timelines to collect attestations from critical software producers. Additionally, M-23-16 provided supplemental guidance to agencies on the use of a Plan of Action and Milestones (POA&M) when a software producer cannot provide the required attestation.

Critical Software

NIST defines critical software as "any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes:

1. Is designed to run with elevated privilege or manage privileges,
2. Has direct or privileged access to networking or computing resources

3. Is designed to control access to data or operational technology,
4. Performs a function critical to trust, or
5. Operates outside of normal trust boundaries with privileged access."[1]

PBGC Departments and Personnel Involved in the Attestation Process

Two departments are responsible for developing PBGC's critical software self-attestation (attestation) efforts. First, the Information Technology Infrastructure Operations Department (ITIOD), within the Office of Information Technology, oversees infrastructure systems and services delivery, ensures service levels are met; and ensures overall business continuity. Second, the Enterprise Cybersecurity Department (ECD), also within the Office of Information Technology, manages all aspects of cybersecurity.

ITIOD and ECD officials determined Service Application Owners (SAO) were in the best position to acquire the public and non-publicly available attestations from the software producers and provide them to ECD officials to review for completeness.[2] ECD officials explained that SAOs were chosen to obtain the attestation forms because they were close to contracting staff, responsible for authorizing system changes, and approved access to the services and applications that are assigned to them by the Information Owner for the *Federal Information Security Modernization Act of 2014* (FISMA) systems they support.

PBGC's Critical Software Inventory

PBGC maintains the Corporation's Critical Software Inventory within ServiceNow fields. The ServiceNow Critical Software Inventory is comprised of custom fields to store data and displays the critical software, among other services, that are associated with each of PBGC's FISMA systems.[3,4] ITIOD personnel explained that the Critical Software

[1] See the critical software definition at https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/critical-software-definition-explanatory.
[2] According to PBGC's *Infrastructure Configuration Management Plan*, an SAO is responsible for managing access to the service information and approves access requests, serving as the subject matter expert and advocating for the service or application, and coordinates and approve IT service/application changes.
[3] Per PBGC's *Infrastructure Configuration Management Plan*, a Business Service is a PBGC Configuration Item (CI), or an identifiable part of a system (see footnote 7 for full definition of a CI). PBGC's *Configuration Management Process* states that the Business Services reflect the applications and services associated with PBGC's FISMA systems. Per PBGC ITIOD personnel, PBGC's hardware and infrastructure components are mapped to PBGC's critical software, which are associated with PBGC's FISMA systems.
[4] PBGC personnel identified that the PBGC's Critical Software Inventory, applicable to Executive Order 14028, are service fields in ServiceNow. The service fields are high-level views of PBGC's system components for each of its FISMA systems. However, the service fields are not a list of PBGC's entire CMDB CIs.

Inventory is integrated into PBGC's Configuration Management (CM) process.[5]

Objective

Our objective was to evaluate PBGC's efforts regarding the software self-attestation requirements.

[5] CM is the set of disciplines and policies used for controlling and managing the CIs of PBGC's Information Technology infrastructure.

Audit Results

Summary

PBGC made some efforts to meet the critical software self-attestation requirements (attestation); specifically, PBGC established a process for the Critical Software Inventory in ServiceNow and obtained and stored some attestations for critical software. However, while PBGC inventoried critical software, the inventory did not contain all data elements needed to verify attestations received for PBGC's software. Instead, PBGC used complex methods to manage and maintain critical software within the ServiceNow inventory, which did not always result in locating data elements. Additionally, we also found instances where the Corporation did not adequately collect, review, and manage attestations; this led to PBGC utilizing critical software that may not meet minimum secure software development requirements.

Finding 1: PBGC Should More Effectively Manage Its Critical Software Inventory

OMB M-22-18 requires agencies create an inventory of all software subject to the requirements therein, with a separate inventory for "critical software." Additionally, M-22-18 and its update, M-23-16; the Cybersecurity and Infrastructure Security Agency (CISA) *Secure Software Development Attestation Form* (SSDAF); NIST; and PBGC personnel, identified requirements for attestations that should be included in the Critical Software Inventory to verify received attestations.

We identified the following 11 data elements for PBGC's Critical Software Inventory necessary to (1) indicate the software was within the scope of M-22-18 and subsequent updates, or was exempt, (2) identify if the software was critical, and (3) verify an attestation was received:

1. PBGC's Business Service
2. Critical Software
3. Operational Status
4. SAOs
5. FISMA System
6. Exemptions
7. Attestation Type
8. Version Number
9. Release/Publish Date
10. Product Name
11. Software Producer

For the source for each data element, see Appendix IV.

Improvements Needed for PBGC's Critical Software Inventory

We found that PBGC's Critical Software Inventory did not identify all 11 data elements; specifically, 6 of 11 data elements were missing from PBGC's Critical Software Inventory:

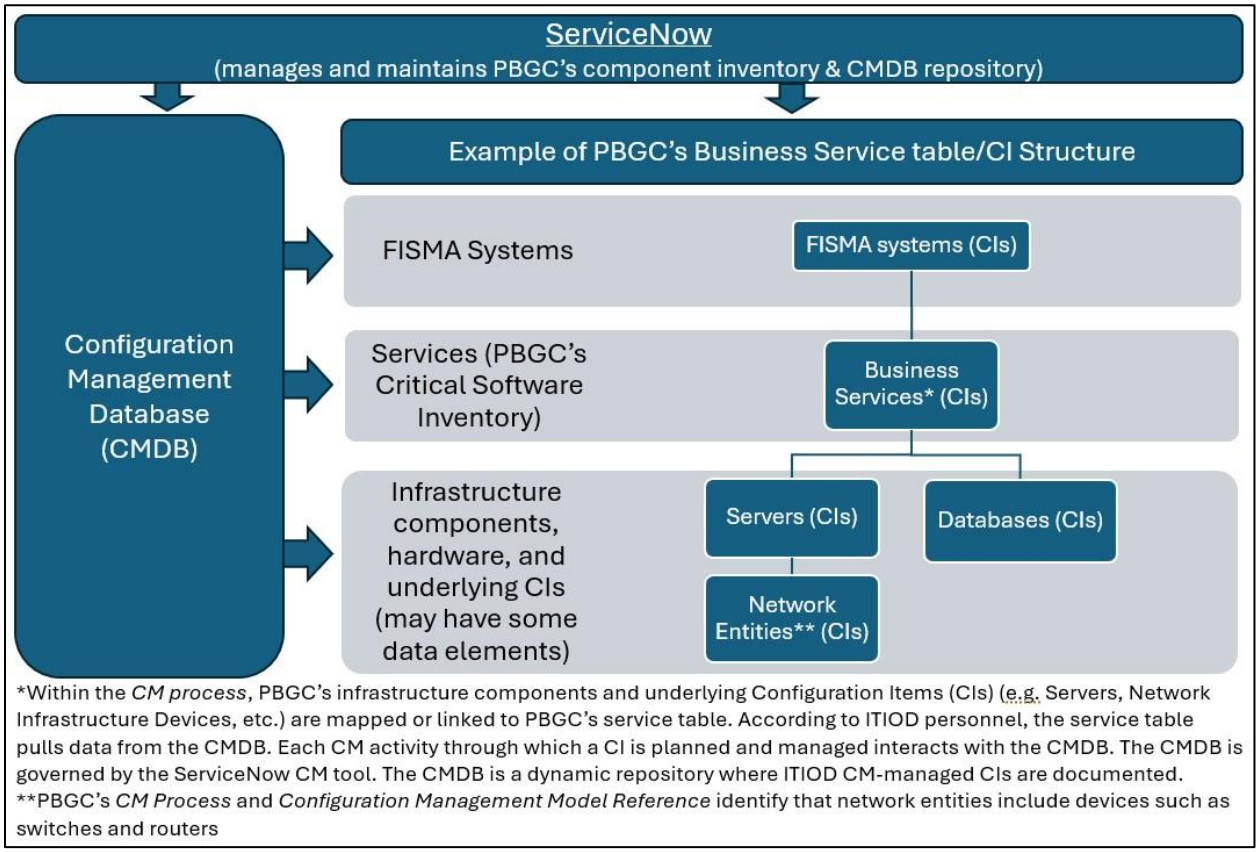
1. Exemptions
2. Attestation Type
3. Version Number
4. Release/Publish Date
5. Product Name
6. Software Producer

As of December 10, 2024, PBGC identified 75 critical software in their Critical Software Inventory.[6] Some of the critical software lacked a data element or the field was blank. In some instances, the critical software names had a variation of a potential product name or software producer. For instance, we found software within the Critical Software Inventory that matched a portion of the product name. In another instance, one critical software displayed the software producer, but there was no product name.

For other data elements, the Corporation used complex methods to manage and maintain its PBGC Critical Software Inventory. PBGC officials identified that not all of the data elements were in one location within the Critical Software Inventory. Officials believed some of the required data elements were in PBGC Critical Software Inventory, but others were at lower-level Configuration Items (CIs)[7] within the structure. See Figure 1 for a depiction of PBGC's Critical Software Inventory Hierarchy. ITIOD further explained that the Critical Software Inventory is integrated into PBGC's CM process and identifying the possible data elements could be done by either: (1) navigating to the *Relationships* tabs and selecting each of the mapped underlying CIs (e.g. servers, network infrastructure devices, etc.) or (2) navigating to the *Change Requests* tabs of the Business Services themselves.[8]

[6] PBGC classifies software as Business Services in their inventory.
[7] A CI is an identifiable part of a system (e.g., hardware, software, firmware, documentation, or a combination thereof) that is a discrete target of configuration control processes within the CM process. CI's include, but are not limited to computers, servers, applications, network components, and databases that PBGC controls.
[8] A user could then find specific information related to a software by navigating to the *Software Installations* tab on the underlying CI mapped to the Business Service. Additionally, a user could search each individual change request listed on the *Change Request* tab for potential data elements in the entry details.

Figure 1. PBGC's Critical Software Inventory Hierarchy



Source: OIG prepared based on PBGC's *Configuration Management Process* and walkthroughs by ITIOD personnel.

We reviewed 23 of the 75 critical software.[9] For our review, we followed the methods PBGC provided to identify potential data elements on the linked CIs or Change Requests. However, we were unable to locate all data elements that were not in the Critical Software Inventory because, in some instances, there were no change request entries on the CIs. Additionally, there were no underlying mapped CIs linked to the critical software.

Additional Resources Needed to Manage the Critical Inventory Process

ECD and ITIOD officials explained they did not initially have resources available to manage the critical inventory process. Further, ITIOD noted that mapping of the underlying CIs was incomplete.

[9] Due to audit limitations and missing data fields, we could not quantify the entire scope of missing or blank data elements.

Additionally, CISA and OMB released the SSDAF on March 11, 2024, approximately eight months before we initiated this audit. As a result of updated requirements, it may take PBGC time to implement the NIST and SSDAF requirements into the Critical Software Inventory. However, without a comprehensive inventory, including the required data elements, PBGC may not be able to determine what critical software is on its network that requires an attestation. A consolidated representation of the data elements and components within the Critical Software Inventory and associated CIs would provide PBGC with a clearer picture and management over critical software. Moreover, it would provide transparency and tracking to show that critical software is properly identified and accounted for.

Recommendation

We recommend that the Office of Information Technology:

1. Update and maintain a complete Critical Software Inventory that staff may utilize to fulfill their responsibilities and provide transparency and tracking.

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OIT stated that it will mature its use of ServiceNow or other tools to ensure tracking and transparency of software attestation data to the appropriate level of detail. OIT's goal is to complete the planned action by July 31, 2026.

Closure of this recommendation will occur when the Corporation provides documentation that it is maintaining a complete Critical Software Inventory that includes the appropriate level of detail for transparency and tracking, which include the data elements identified in the finding.

Finding 2: PBGC Must Better Manage its Attestation Process

Public Law 115-390, the *Secure Technology Act*, and NIST Special Publication 800-53, *Security and Privacy Controls for Information Systems and Organizations*, require federal agencies to develop supply chain risk management policies and procedures. Additionally, OMB M-22-18 and M-23-16 required agencies to collect attestation letters for "critical software" by June 8, 2024. M-22-18 and M-23-16 also require agencies to ensure software producers identify in the form secure practices they cannot attest to, submit POA&Ms for those risks, and document practices in place to mitigate associated risks.[10] Agencies must discontinue use of the software if the producer's documentation

[10] NIST defines a POA&M as a document that identifies tasks, resources, milestones, and scheduled completion dates.

is found unsatisfactory. Further, when an attestation is not provided, agencies are responsible for requesting an OMB extension for continued use.

OMB M-22-18 also requires the Chief Information Officer to develop training plans for the review and validation of software attestations and artifacts. According to the SSDAF instructions, agencies must ensure all fields in the attestation are appropriately completed by the software producer because incomplete forms cannot be accepted. M-22-18, also allows the software producer to choose to demonstrate conformance by submitting an assessment from a Third-Party Assessor Organization to the agency. To rely upon a Third-Party Assessor Organization, the software producer must check the appropriate box in the attestation and attach the assessment to the form.

Based on the elements outlined in OMB M-22-18, M-23-16, and the SSDAF, we identified the following attributes to determine the completeness of the attestations:

- Software Producer Information;
- Product Name;
- Attestation Submission Date;
- Description of Software;
- Acknowledgement of Attestation Statement;
- Acknowledgement of Third-Party Assessor Organization and Attached Artifacts, if applicable;
- Signature of Chief Executive Officer or Designee; and
- Other Attachments, such as a POA&M, if applicable.

PBGC Needs Stronger Oversight of its Attestation Efforts

PBGC did not collect all attestations by the required OMB M-22-18 and M-23-16 due dates. PBGC officials informed us that the Corporation had 22 outstanding critical software products. Further, we found nine other attestations were submitted to PBGC after OMB's collection due date.

We identified 26 attestations in PBGC's Cyber Security Assessment and Management (CSAM) Application and CISA's Repository for Software Attestations and Artifacts. However, we were unable to verify the total number of critical software with an attestation in PBGC's possession because vendors did not always include a software product's name in its Critical Software Inventory (see Finding 1). In addition, when discussing with PBGC how they matched the Critical Software Inventory to the attestations, officials stated, "I would like to say, that – the numbers don't always make sense" (i.e. the totals between ServiceNow and CSAM do not always match). Due to the inability to quantify the critical software obtained and PBGC's disclaimer, we have

concluded that the true number of critical software products with attestations is unknown to the Corporation.

Additionally, according to an ECD official, the Department reviewed attestations for completeness after collection from the SAOs, who were responsible for acquiring the attestations from software producers and CISA's Repository for Software Attestations and Artifacts. Some of the SAOs interviewed did not perform reviews or identify deficiencies within the attestations before providing them to ECD for review and storage. Further, while an ECD official stated they reviewed the software version, OMB control number, and expiration date, we found issues in most cases with the completeness of the attestations even after review.

Of the 26 attestations we reviewed,16 were not completed in accordance with attestation instructions. Figure 2 illustrates issues with the attestations we reviewed.

Figure 2: Issues with the Review of Attestations

Software Producer	Submitted After Attestation Due Date	Description of Software	Self-Attestation Statement	Third-Party Assessor Organization	Attached Third-Party Assessor Organization Assessment	CEO or Designee Signature	Complete Attestation Package
1						NA	
2	X			NA			X
3				NA			
4	X					NA	X
5	X	X				NA	X
6				NA			
7	X			NA			X
8	Unknown	X	X	Unknown		X	X
9			X	NA			X
10	X		X	NA			X
11	Unknown	X	X		X	NA	X
12	Unknown		X		X	NA	X
13			X	NA			X
14				NA			
15	Unknown	Unknown	Unknown	Unknown		Unknown	
16	X			NA			
17	Unknown	X	X		X	NA	X
18				NA			
19		X				NA	X
20				NA			
21	X					NA	X
22				NA			
23	Unknown	NA	X		X	NA	X
24	Unknown	Unknown		Unknown		X	X
25	X	Unknown	X		X	NA	X
26	X	NA		NA			
Total	9	5	9		5	2	16

Source: OIG prepared based on review of attestations.

Key

- X – Did not meet criteria element.
- Unknown – Information not available.
- NA – Does not apply.
- Blank Spaces – Information present and met criteria element.

We also found two software producers who could not attest to adhering to all secure software development practices. One producer identified practices to which they could not attest and provided a POA&M, but they did not document the practices they have in place to mitigate associated risks to PBGC. Another identified the practices to which they could not attest, but did not submit a POA&M or document practices they have in place to mitigate associated risks. Despite these things, PBGC continues to use these critical software products and has not received any further guidance from OMB. PBGC officials stated the first software producer provided an update in December 2024, stating they will complete their work by December 2025. PBGC has contacted the other software producer and PBGC will continue to track.

For outstanding attestations, PBGC officials created POA&Ms and said they intend to accept the risks. Although PBGC requires monthly POA&M monitoring, there was a lack of evidence that the Corporation periodically reviewed the open attestation POA&Ms. PBGC stated they are awaiting further guidance from OMB on extensions and waivers.

Additional Efforts Necessary for PBGC's Attestations

While executing the attestation process, PBGC did not develop or incorporate all requirements into formal policies or procedures for the staff responsible to ensure staff understood the requirements of the work and performed consistently. The Corporation also believed they had incorporated the review and validation of attestations and artifacts into general training; however they had not. Another challenge according to PBGC officials is due to software producer delays in responding or not providing complete forms, which resulted in some untimely or incomplete attestations. They believe, as a small agency, PBGC does not have the leverage to ensure software producers fully meet SSDAF requirements.

Additionally, *PBGC's POA&M Process* guidance was not updated to reflect OMB M-22-18 and M-23-16 instructions regarding how to review, obtain, or remediate software producers' POA&Ms that have identified practices that cannot be attested. And while the Corporation plans to accept the risk of using critical software that has not been attested to, risk acceptance is still only in draft form. Further, PBGC stated that Executive Order 14144, *Strengthening and Promoting Innovation in the Nation's Cybersecurity*, introduces additional supply chain security measures, including a requirement that software producers submit attestations to CISA. However, PBGC is waiting for guidance regarding the requirement as the process is not efficient for attestations to support critical government services.

As a result, PBGC is not fully compliant with the OMB guidance and the quality and completeness of the attestation program is insufficient. Without guidance and training for the attestation process, when new software is attained or designated, the

Corporation may not be able to properly examine and confirm the accuracy of attestations. PBGC also risks an incomplete understanding of its compliance with the minimum secure software development requirements and increases the chances of inaccurate POA&Ms leading to improper remediation actions to correct and reduce weaknesses.

Recommendations

We recommend that the Office of Information Technology:

2. Create or update guidance to implement policies and procedures to guide and govern supply chain risk management activities related to attestations.

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OIT stated that it will update both the Software Attestation Standard Operating Procedure to clearly address attestation procedures and include reviews of POA&Ms, as well as the Cybersecurity-Supply Chain Risk Management Implementation Plan, Strategy, and Overview. Further, OIT will monitor and update its policies and procedures given a recent Executive Order, issued on June 6, 2025, that modifies existing and future software attestation requirements. OIT's goal is to complete the planned action by March 31, 2026.

Closure of this recommendation will occur when the Corporation provides the updated guidance to implement policies and procedures to guide and govern supply chain risk management activities related to attestations.

3. Ensure all responsible staff receive appropriate training on attestation roles and responsibilities.

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OIT stated that it will more definitively define roles and responsibilities with respect to software attestation and ensure that those staff are appropriately trained regarding their respective responsibilities. OIT's goal is to complete the planned action by July 31, 2026.

Closure of this recommendation will occur when the Corporation provides documentation that it has defined roles and responsibilities for responsible staff and provided appropriate training.

4. Update PBGC's process documentation to properly align with OMB requirements for software producers who cannot attest to adhering to the secure software

development practices within their attestations and ensure PBGC effectively follows this process.

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OIT stated that it will follow the Risk Management Framework Process and Enterprise Plan of Actions and Milestones Process to ensure any missing attestations are addressed. While OIT's response did not identify that it would update existing PBGC process documentation, OIT identified that a recent Executive Order on June 6, 2025 modifies existing and future software attestation requirements and OIT will update requirements accordingly. OIT's goal is to complete the planned action by December 31, 2025.

Closure of this recommendation will occur when the Corporation provides updated documentation that properly aligns with OMB requirements, including any updates from the Executive Order for software producers who cannot attest to adhering to the secure software development practices within their attestations, and documentation that PBGC is following the process.

5. Contact OMB to obtain additional guidance to determine if an exception, waiver, or if the Corporation should discontinue the use of software for outstanding attestations.

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OIT stated, in light of a recent Executive Order on June 6, 2025 that modifies existing and future software attestation requirements, it will reach out to OMB for updated guidance on the process for collection of attestation and guidance regarding the use of software for missing attestations. OIT's goal is to complete the planned action by December 31, 2025.

Closure of this recommendation will occur when the Corporation provides documentation that it has received additional guidance from OMB regarding exceptions, waivers, or if the Corporation should discontinue the use of software for outstanding attestations and has implemented the additional guidance.

Appendix I: Objective, Scope, Methodology, and Standards

Objective

Our objective was to evaluate PBGC's efforts regarding the software self-attestation requirements.

Scope

Our scope included assessing PBGC's management and implementation of its software attestation process. We conducted this audit from our office at PBGC headquarters, 445 12th Street SW, Washington, DC 20024. We conducted fieldwork from November 2024 to April 2025.

Our review focused on critical software.

Due to the size of CMDB, our audit attestation scope, and time limitations, our review focused on identifying areas for possible improvement related to PBGC's Critical Software Inventory. Further, due to audit limitations and missing data fields, we could not quantify the entire scope of missing or blank data elements.

Methodology

To answer our objective, we reviewed applicable OMB, NIST, CISA, the *Secure Technology Act*, and PBGC criteria. We interviewed PBGC officials for additional information. In addition, we reviewed documentation from PBGC officials, including critical inventory, PBGC guidance, attestation training, attestations, and an extension request sent to OMB.

Use of Computer Processed Data

We relied on computer processed data extracted from CSAM, data from ECD, and Critical Software Inventory in ServiceNow. To assess the reliability of computer processed data from the CSAM, data from ECD, and Critical Software Inventory in ServiceNow, we conducted a series of tests to: (1) ensure that we received all computer processed data needed to fully assess PBGC's efforts regarding attestation process, and (2) determine if that data was sufficient and reliable by checking if it was complete and accurate, but only for the purposes of determining whether we were looking at all available data PBGC used in their attestation review. These tests included: (1) our

retrieval of CSAM data (2) Critical Software Inventory in ServiceNow documentation from the systems and our requests, and (3) data from PBGC personnel, such as the spreadsheets from ECD. This was to ensure the audit team had all available information related to PBGC's review of the attestation process requirements. Then, we conducted a check to ensure the data was complete, accurate, and had all documents available for our review.

We determined the data was sufficient, appropriate, and reliable for our purposes, which included looking at all available documentation PBGC maintained for their efforts regarding the software self-attestation process.

Assessment of Internal Controls

We assessed internal controls and compliance with laws and regulations necessary to satisfy the audit objective. In particular, we assessed the internal control components and underlying principles significant to the audit objectives. However, because our review was limited to these internal control components and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Applicable Professional Standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Agency Response

Pension Benefit Guaranty Corporation

445 12th Street SW
Washington, DC 20024-2101
202-229-4000
PBGC.gov

July 11, 2025

TO: John Seger
Assistant Inspector General for Audits, Evaluations, and Inspections

FROM: Bob Scherer
Chief Information Officer

ROBERT SCHERER
Digitally signed by ROBERT SCHERER
Date: 2025.07.10 17:00:39 -04'00'

SUBJECT: Management Response to OIG's Draft Report, PBGC's Self-Attestation Efforts (Project No. PA-25-185)

Thank you for the opportunity to comment on the Office of Inspector General's (OIG) draft report, received June 26, 2025, relating to the evaluation of Pension Benefit Guaranty Corporation's (PBGC) efforts regarding the software self-attestation requirements. Your office's work on this is sincerely appreciated.

PBGC management met with the representatives from the OIG on June 23, 2025, to discuss the findings and recommendations. The dialogue was both informative and insightful and PBGC is grateful for the opportunity to respond to the recommendations suggested by the OIG.

Management concurs with the report's findings and recommendations. In the attachment to this memorandum, you will find our specific responses to each recommendation and scheduled completion dates. Addressing these recommendations in a timely manner is an important priority for PBGC.

Attachment

cc: Alice Maroni, Acting Director
Karen Morris, General Counsel
Damon McClure, Director, Procurement Department
Lisa Carter, Acting Chief Financial Officer/Director, Corporate Controls and Reviews Department
Latreece Wade, Risk Management Officer

Our comments on the specific recommendations in the draft report are as follows:

1. **Update and maintain a complete Critical Software Inventory that staff may utilize to fulfill their responsibilities and provide transparency and tracking. (OIG Control Number 2025-10-01-OIT)**

PBGC Response: Management concurs with this recommendation. The Office of Information Technology (OIT) will mature its use of ServiceNow or other tools to ensure tracking and transparency of software attestation data to the appropriate level of detail.

Scheduled Completion Date: July 31, 2026

2. **Create or update guidance to implement policies and procedures to guide and govern supply chain risk management activities related to attestations. (OIG Control Number 2025-10-02-OIT)**

PBGC Response: Management concurs with this recommendation. OIT will update the Software Attestation Standard Operating Procedure (SOP) to clearly address attestation procedures. Additionally, the Cybersecurity-Supply Chain Risk Management (C-SCRM) Implementation Plan, Strategy, and Overview (IPSO), which includes software attestation as a critical success factor for compliance and integration with procurement, will be updated as necessary. ECD also maintains a Plan of Actions and Milestones (POA&M) dashboard and reviews them at each staff meeting, including those related to software attestation. The Software Attestation SOP will be updated to include review of POA&Ms.

On June 6, 2025, President Trump issued a recent Executive Order that modifies existing and future software attestation requirements. OIT will monitor that and update our policies and procedures accordingly.

Scheduled Completion Date: March 31, 2026

3. **Ensure all responsible staff receive appropriate training on attestation roles and responsibilities. (OIG Control Number 2025-10-03-OIT)**

PBGC Response: Management concurs with this recommendation. OIT will more definitively define roles and responsibilities with respect to software attestation and ensure that those staff are appropriately trained regarding their respective responsibilities.

Scheduled Completion Date: July 31, 2026

4. **Update PBGC's process documentation to properly align with OMB requirements for software producers who cannot attest to adhering to the secure software development practices within their attestations and ensure PBGC effectively follows this process. (OIG Control Number 2025-10-04-OIT)**

PBGC Response: Management concurs with this recommendation. OIT will follow the Risk Management Framework (RMF) Process and Enterprise Plan of Actions and Milestones Process (POA&M Process) to ensure any missing attestations are addressed. Additionally, on June 6, 2025, President Trump issued a recent Executive Order that modifies existing and future software attestation requirements. OIT will monitor actions and update requirements accordingly.

Scheduled Completion Date: December 31, 2025

5. **Contact OMB to obtain additional guidance to determine if an exception, waiver, or if the Corporation should discontinue the use of software for outstanding attestations. (OIG Control Number 2025-10-05-OIT)**

PBGC Response: Management concurs with this recommendation. In light of President Trump's June 6, 2025, Executive Order, OIT will continue to reach out to OMB for updated guidance on the process for collection of attestation and guidance regarding the use of software for missing attestations.

Scheduled Completion Date: December 31, 2025

Appendix III: Acronyms

Acronym	Meaning
Attestation	Critical Software Self-Attestation
CI	Configuration Item
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CMDB	Configuration Management Database
CSAM	Cyber Security Assessment and Management Application
ECD	Enterprise Cybersecurity Department
FISMA	Federal Information Security Modernization Act of 2014
ITIOD	Information Technology Infrastructure Operations Department
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PBGC or the Corporation	Pension Benefit Guaranty Corporation
POA&M	Plan of Action and Milestones
SAO	Service Application Owners
SSDAF	Secure Software Development Attestation Form

Appendix IV: Data Elements

Based on OMB M-22-18, M-23-16, SSDAF, NIST definition of critical software, and discussions with PBGC personnel, we identified a total of 11 data elements needed in the PBGC's Critical Software Inventory to: (1) determine if the software was within the scope of the M-22-18 requirements or was exempt, (2) identify if the software was critical and (3) verify an attestation was received. These data elements are provided below, along with the justification for having the data element or source of the requirement:

#	Data Element	Description	Reference
1.	**PBGC's Business Service**	PBGC personnel identified that the inventory of PBGC's Critical Software Attestations, applicable to Executive Order 14028, are ServiceNow fields, which are made up of PBGC's Business Services.	Walkthrough with PBGC Officials
2.	**Critical Software**	Agencies shall inventory all software subject to the requirements of the memorandum, with a separate inventory for "critical software."	M-22-18
3.	**Operational Status**	PBGC personnel identified the operational status shows whether the service is operating on PBGC's systems.	Walkthrough with PBGC Officials
		The NIST definition of critical software states it applies to software of all forms (e.g., standalone software, software integral to specific devices or hardware components, cloud-based software) purchased for, or deployed in, production systems and used for operational purposes. Other use cases, such as software solely used for research or testing that is not deployed in production systems, are outside of the scope of the definition.	NIST Definition of Critical Software
4.	**SAOs**	The SAO is responsible for obtaining the attestation from vendors.	Walkthrough with PBGC Officials
5.	**FISMA System**	Attestations are stored within CSAM under the FISMA system associated with the PBGC critical software.	Walkthrough with PBGC Officials
6.	**Exemptions**	OMB M-22-18, and its subsequent updates, identify certain exemptions for obtaining an attestation. For example, OMB M-23-16 states agencies are not required	OMB M-22-18 OMB M-23-16 SSDAF

		to collect attestations for products that are freely obtained and publicly available.	
7.	**Attestation Type**	The attestation can be Company-wide, for an Individual Product, or for Multiple Products or Specific Product Version(s).	SSDAF
8.	**Version Number**	If the attestation is for an individual product or multiple products, provide the version number to which the attestation applies. Updated forms are not required for future versions of products if the software producer's development practices conform to the security practices outlined in their attestation.	SSDAF
9.	**Release/Publish Date**	If the attestation is for an individual product or multiple products, provide the release/publish date to which the attestation applies.	SSDAF
10	**Product Name**	If the attestation is for an individual product or multiple products, provide the complete name to which the attestation applies.	SSDAF
11.	**Software Producer**	Agencies must obtain an attestation from the software producer before using the software, or the software producer can provide a third-party assessment.	OMB M-22-18 OMB M-23-16 SSDAF

Appendix V: Staff Acknowledgments

Staff Acknowledgements	John Seger, Assistant Inspector General for Audits, Evaluations, and Inspections; Marcie McIsaac, Audit Manager; Kelly Migliore, Auditor-in-Charge; Bryan Beardsley, Auditor; and Tiara Grotte, Auditor, made key contributions to this report.

Appendix VI: Feedback

Please send your comments, suggestions, and feedback to OIGFeedback@pbgc.gov and include your name, contact information, and the report number. You may also mail comments to us:

Office of Inspector General
Pension Benefit Guaranty Corporation
445 12th Street SW
Washington, DC 20024-2101

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 326-4030.