



OFFICE OF INSPECTOR GENERAL EVALUATION REPORT

PBGC's Data Protection at Contractor-Operated Facilities

**Report No. EVAL-2019-08
January 31, 2019**

PBGC's Data Protection at Contractor-Operated Facilities

Background	<p>\$5.8 billion. The amount PBGC paid in benefit payments during Fiscal Year 2018 to more than 861,000 retirees.</p> <p>Office of Benefits Administration (OBA). The PBGC office that manages the termination process for defined-benefit plans and provides participant services.</p> <p>Contractor-Operated Facilities. Field offices that support OBA and perform benefits administration duties for the approximate 1.4 million participants.</p> <p>Office of Management and Administration (OMA). The PBGC office that provides personnel and physical security-related services to PBGC federal employees and contractors.</p> <p>Public Trust Agency. Contractors and federal employees must be properly vetted due to the nature of PBGC's business of dealing with a large volume of personally identifiable information (PII).</p>
Risks	<p>Risk. Ineffective or non-existent controls increase the risk of leakage, theft, loss or unauthorized disclosure of sensitive participant data.</p>
Key Questions	<p>Evaluation Objective. Determine whether controls relating to data protection are suitably designed and operating effectively at contractor-operated facilities.</p>
Evaluation Results	<p>Overall Conclusion. We found controls relating to data protection at the contractor-operated facilities are, for the most part, suitably designed. However, PBGC has opportunities to improve the operational effectiveness of some of these controls. Specifically, we found:</p> <ul style="list-style-type: none"> • Controls relating to monitoring of the personnel security process and oversight by the Contracting Officer's Representatives (CORs) are not consistently executed in a manner to ensure protection of sensitive data. • Vulnerabilities in the employee separation process that require additional controls. <p>Employee Vetting. We reviewed records of 65 contractor employees. We found missing data for 7 "required" fields in PBGC's background investigation and security clearance system and found the fields contained no data for 5 to 54 percent of the contractor employees in our sample. We found no records for 2 of the 65 contractor employees. In addition, we found instances where PBGC did not meet its established milestones, ranging from 46 to 97 percent, to complete various personnel security actions.</p> <p>CORs. We found a lack of vigilance resulting in varying PII practices, weaknesses in physical access restrictions at field offices, and untimely employee separation actions.</p>
Corrective Actions	<p>Our recommendations. We made eight recommendations to management to improve monitoring and management oversight of the personnel security process, the COR oversight function at contractor-operated facilities, and controls over the employee separation process.</p> <p>Management agreement. Management agreed with the eight recommendations and agreed to take corrective action as identified in the report.</p>



Office of Inspector General
Pension Benefit Guaranty Corporation

January 31, 2019

TO: David Foley
Chief of Benefits Administration

Alice Maroni
Chief Management Officer

FROM: Brooke Holmes 
Assistant Inspector General for Audit

SUBJECT: Issuance of Final Evaluation Report No. EVAL-2019-08
PBGC's Data Protection at Contractor-Operated Facilities

We are pleased to provide you with the above-referenced evaluation report. We appreciate the cooperation you and your staff extended to 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: Frank Pace, Acting Director, Corporate Controls and Reviews Department
Latreece Wade, Acting Risk Management Officer
Judith Starr, General Counsel
Department of Labor Board staff
Department of the Treasury Board staff
Department of Commerce Board staff
House committee staff (Education and Workforce, Ways and Means, HOCR)
Senate committee staff (HELP, Finance, HSGAC)

Table of Contents

Background	2
Evaluation Results	5
Finding 1: PBGC Needs to Improve Monitoring and Management Oversight of the Personnel Security Process.....	5
Recommendations.....	8
Finding 2: PBGC Needs to Improve the COR Oversight Function at Contractor-Operated Facilities	10
Recommendations.....	14
Finding 3: PBGC Needs to Improve Controls over Employee Separation Process	15
Recommendations.....	18
Other Matters	19
Appendix I: Objective, Scope, and Methodology	20
Appendix II: Agency Response	22
Appendix III: Acronyms	27
Appendix IV: Staff Acknowledgements	28
Appendix V: Feedback	29

Background

Pension Benefit Guaranty Corporation

Congress established the Pension Benefit Guaranty Corporation (PBGC) through the Employee Retirement Income Security Act of 1974 to insure the defined-benefit pensions of workers and retirees in private-sector pension plans. PBGC insures two types of defined-benefit plans in two separate insurance programs: single-employer and multiemployer. Through these two programs, PBGC protects the retirement security of nearly 37 million American workers, retirees, and their families in more than 25,000 pension plans. PBGC finances its operations through insurance premiums set by Congress and paid by sponsors of PBGC-insured pension plans, as well as investment income, assets from pension plans trusted by PBGC, and recoveries from the companies formerly responsible for the plans.

Office of Benefits Administration

The Office of Benefits Administration (OBA) manages the termination process for defined-benefit plans and provides participant services (including calculation and payment of benefits) for PBGC-trusted plans. In FY 2018, OBA paid benefits payments of \$5.8 billion to more than 861,000 retirees from 4,919 failed single-employer plans. An additional 532,000 retirees are scheduled to receive their benefits from PBGC when they retire.

Contractor-Operated Facilities Providing Benefits Administration

OBA uses contractor-operated facilities in four field offices to perform benefits administration duties for the approximate 1.4 million participants receiving benefits or scheduled to receive benefits from PBGC when they retire. Currently, there are three Field Benefits Administration (FBA) offices: Coraopolis, PA; Miami, FL; and Wilmington, DE. The FBAs are responsible for processing the active inventory of approximately 500 plans in the valuation and benefit determination process. The fourth contractor-operated field office is located in Euclid, OH (previously, this office was located in Richmond Heights, OH). This office is a Post Valuation Administration (PVA) field office that administers benefits for over 4,000 plans for which final benefit determinations have been issued.

OBA uses a contractor-operated facility in Kingstowne, VA, for customer support and document management. The Customer Contact Center (CCC) serves as the initial point of contact for the public and pension benefit participants. Customer Service Representatives serve participants who call the CCC with benefit-related questions and requests regarding their PBGC pensions

and account profiles. Customer Service Representatives also transfer calls to PBGC staff and the appropriate FBA points of contact, who assist the participant with benefit-specific questions and requests. The Document Management Center (DMC) provides document and records management support to PBGC.

On a daily basis, contractor employees at these offices are accessing, viewing, and updating personally identifiable information (PII) as part of their duties. All PBGC employees and contractors are responsible for protecting sensitive information—including PII—in accordance with law and PBGC policy. The OBA Contracting Officer's Representatives (CORs) are responsible for monitoring the progress of the contractor's work to ensure the contractor is meeting all contract requirements, including the protection of PII in accordance with law and policy.

Personnel and Physical Security

Within PBGC, the Office of Management and Administration (OMA) provides personnel and physical security-related services to PBGC federal employees and contractors. This includes:

- PIV credentialing;
- Personnel security and suitability screening;
- Physical security access; and
- Workplace security incidents.

Personnel Suitability

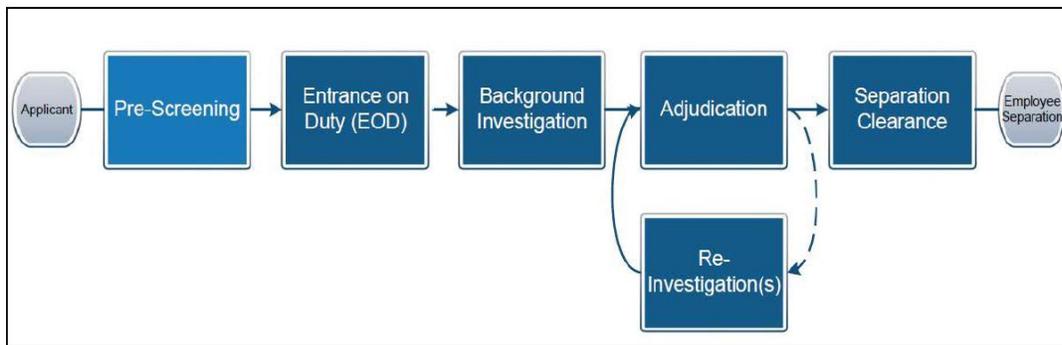
PBGC is a Public Trust agency, and all background investigations are at the Public Trust level, unless otherwise specified. Background investigations for PBGC federal and contractor employees are conducted by the OPM National Background Investigations Bureau. Within OMA, security specialists are responsible for the intake process and ensuring that all relevant personal and candidate information is added to the Personnel Security Investigation Solution system (PSIS), PBGC's web-based and cloud-hosted, background investigation and security clearance application. The security specialist initiates a background investigation upon completion of entrance-on-duty (EOD) security processing for contractor employees. The background investigation is initiated and submitted via OPM's Electronic Questionnaire for Investigative Processing (e-QIP) system.

PBGC Directive PM 05-17, *Personnel Security and Suitability Program* (August 30, 2018), details the roles and responsibilities to designate position risk levels, initiate security processing for onboarding and separating federal and contractor employees, and adjudicating the suitability or fitness of all federal and contractor employees. The *Personnel Security Standard Operating*

Procedures (SOP) (December 6, 2016) detail the procedures to be followed by all federal and contractor employees. It is PBGC's policy to employ only those persons who are found to be suitable or fit for employment. Pre-screening is the process by which an applicant is fingerprinted and a Special Agreement Check is completed before a start date is conveyed. Pre-screening identifies preliminary suitability or fitness issues before an applicant is granted access to PBGC facilities, systems, or information.

The phases of the personnel security process are shown in Figure 1. The SOP assigns the key roles and responsibilities for each phase. Personnel security processing information is captured in PSIS.

Figure 1. Personnel Security Process



Source: PBGC's *Personnel Security SOP*, December 6, 2016.

Objective

We conducted this evaluation to determine whether controls relating to data protection are suitably designed and operating effectively at contractor-operated facilities.

Evaluation Results

Summary

We found controls relating to data protection are, for the most part, suitably designed to protect sensitive information at contractor-operated PBGC facilities. At the same time, PBGC has opportunities to improve the operational effectiveness of some of these controls. We found controls relating to the monitoring of the personnel security process and oversight by Contracting Officer's Representatives (CORs) are not consistently executed in a manner to ensure the protection of sensitive information. We identified vulnerabilities in the employee separation process that require additional controls. Ineffective or non-existent controls increase the risk of leakage, theft, loss or unauthorized disclosure of sensitive participant data. Such events could potentially create benefit payment delays and inefficiencies and can lead to the loss of confidence and trust by stakeholders.

Finding 1: PBGC Needs to Improve Monitoring and Management Oversight of the Personnel Security Process

According to the Government Accountability Office (GAO) *Standards for Internal Control in the Federal Government* (2014), "Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results." The *Personnel Security SOP* provides a process detailing the roles and responsibilities to designate position risk levels, to complete security processing for onboarding and separating federal employees and contractors, and to initiate and adjudicate background and re-investigations. PBGC's Directive IM 15-03, *PBGC Records Management Program* (August 17, 2015), requires all PBGC and contractor employees to identify records received or created, and ensure they remain reliable and usable. Under the *Personnel Security Investigation Solution's (PSIS) Application User Guide*, security specialists are responsible for the intake process and ensuring that all relevant personal and candidate information is added to PSIS and ready for processing.

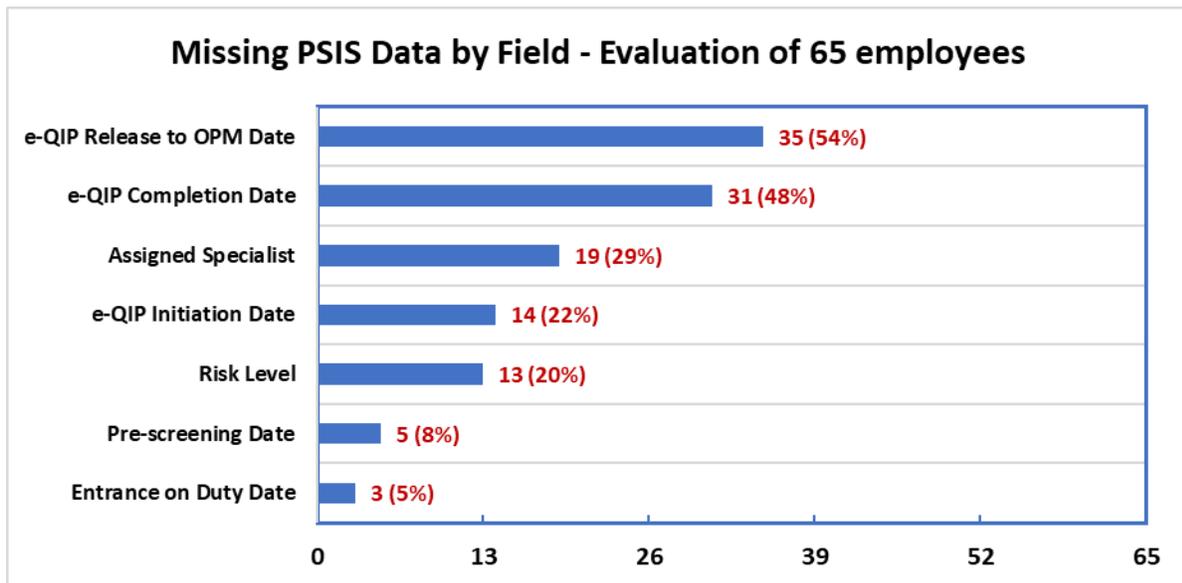
The PSIS application was launched in November 2017. It is used by PBGC security staff to update and query information about employees and contractors to track the status of background investigations and security clearances. The application's business processes and functionality were configured and tailored to meet the needs of the PBGC.

Missing Data in the Personnel Security Investigation Solution System

We reviewed PSIS records relating to all 65 contractor employees who onboarded at the Kingstowne, Miami, and Richmond Heights offices during the period under review.

We found missing data for 7 “required” PSIS fields and found the fields contained no data for 5 to 54 percent of the contractor employees in our sample (Figure 2). In addition, we found no PSIS records for 2 of the 65 contractor employees.

Figure 2. Summary of OIG Observations regarding Missing PSIS Data Fields



Source: OIG analysis of PSIS system for 65 contractor employees.

At our request, PBGC subsequently provided the data related to e-QIP Completion Date and e-QIP Release to OPM Date. While this missing data was retrieved from OPM’s e-QIP system, this data was nevertheless not entered timely in PSIS. For the two contractor employees with no PSIS record, the security team explained that one was terminated, and the other was not properly merged from the old tracking database (PI Manager). According to PBGC management, the information gaps we observed in PSIS was due to the implementation of a new system and personnel workload challenges.

The failure to accurately enter data in PSIS has a compounding effect on processing further down the chain. For example, if data is missing in PSIS for one step in OPM’s e-QIP system, then data for subsequent, dependent steps will also be missing as a result. The e-QIP release step, for example, is dependent upon the completion step, which in turn is dependent upon the

initiation step. If data for initiation is missing, that triggers a cascading data collection failure along successive, dependent steps.

Missed Personnel Security Milestones

In addition to missing data, we found instances where PBGC did not meet its established milestones to complete personnel security actions for contractor employees.

Pre-screening decision date after entrance on duty: Entrance-on-duty (EOD) is the second phase of the personnel security process. The *PSIS Application User Guide* specifies that entrance-on-duty is scheduled if the pre-screening decision is “favorable or favorable with mitigating circumstances.” This action is initiated by the COR after notification of completion of pre-screening from a security specialist. We found that out of 57 contractor employees with available data in PSIS, the pre-screening decision dates were recorded *after* employee’s EOD date in 56 instances (or 97 percent). According to the PBGC security team, the employees get their EOD dates only after PBGC receives favorable fingerprint results. We were able to independently verify this assertion with PSIS data. The recorded pre-screening decision dates were not in line with PBGC established guidelines.

Delays in Electronic Questionnaire for Investigative Processing (e-QIP): Incoming employee background investigations are conducted via OPM’s e-QIP system. According to the *Personnel Security SOP*, the PBGC Security team is responsible for initiating an investigation in the e-QIP system, reviewing the contractor employee’s e-QIP questionnaire for completeness and accuracy, following up with the contractor employee if necessary, and submitting the questionnaire to OPM for background investigation. We found PBGC missed milestones relating to the e-QIP initiation, completion, and release to OPM dates:

- *e-QIP Initiation:* The PBGC Security team informed us that they use 48 hours after EOD date as the milestone for e-QIP initiation of investigations. We found e-QIP initiation was delayed for 34 out of 49 (or 69 percent) contractor employees we evaluated who had available data in PSIS. The delays ranged from 8 to 98 days.
- *e-QIP Completion:* The *Personnel Security SOP* requires contractor employees to complete the e-QIP questionnaire within 14 calendar days from its initiation by PBGC. We found the completion dates for 17 out of 32 contractor employees (53 percent) were past 14 days, ranging from 15 to 136 days after e-QIP initiation dates.
- *e-QIP Release to OPM:* The *PSIS Application User Guide* specifies that the e-QIP Release Due Date is 7 business days after the applicant e-QIP completion date. The e-QIP release dates for 13 out of 28 contractor employees (46 percent) were past 7 business days,

ranging from 13 to 91 days. *(Note: The denominator of contractor employees decreases with each step due to the cascade effect described in the section above.)*

PBGC officials explained that the failure to meet established milestones was due to system limitations during implementation and personnel workload challenges. Missing PSIS data and missed deadlines increase the risk of contractor employees not being properly vetted prior to and after accessing PBGC facilities and systems and exposes PBGC to the risk of leakage, loss or unauthorized disclosure of sensitive information.

Recommendations

We recommend that the Office of Management and Administration:

1. **Evaluate the effectiveness of the current Personnel Security Investigation Solution system and enhance the system functionality as necessary to ensure compliance with the PBGC policies. (OIG Control Number OMA-2)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation and provided ongoing system enhancements that will improve the accuracy of the system. Additionally, OMA stated that since the enhancements, Personnel Security's priority in FY19 is to ensure all data within PSIS is complete and to continue to look for efficiencies to enhance the system. OMA's goal is to complete the system enhancements by March 31, 2021.

Closure of this recommendation will occur when PBGC provides evidence of completed system enhancements and demonstrates their effectiveness in ensuring compliance with PBGC's policies and procedures.

2. **Evaluate the existing employee vetting and security policies to ensure the policies and procedures reflect realistic deadlines. (OIG Control Number OMA-3)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OMA stated that Human Resources Department (HRD) is in the process of updating their Standard Operating Procedures (SOPs) to properly align with actual completion timeframes. In addition, OMA stated that they implemented steps to monitor completion of the background investigation questionnaire for new hires and employees. For contractors, who do not complete the questionnaire, OMA will have the COR remove the contractor for failure to

comply with PBGC Directive PM 05-17. OMA intends to complete the SOP updates by September 30, 2019.

Closure of this recommendation will occur when PBGC provides evidence that the existing policies were updated and properly aligned with realistic completion dates.

- 3. Develop and deliver training for personnel using Personnel Security Investigation Solution application to enhance understanding of the existing policy and requirements. (OIG Control Number OMA-4)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OMA stated that PSIS training sessions covering various topics have been informally delivered to the Personnel Security team in one-on-one and group formats. The updated PSIS user guides also have been distributed to the Personnel Security Team as a reference document. In addition, OMA is in contact with the vendor to conduct formal training sessions for staff. OMA will complete formal training sessions for staff by April 30, 2019.

Closure of this recommendation will occur when PBGC provides evidence that training has been delivered to staff using the PSIS system, relating to PSIS policies and procedures.

- 4. Develop a control to ensure PSIS information is complete, accurate, and timely. (OIG Control Number OMA-5)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OMA stated that the HRD has established weekly and monthly quality checks of new personnel information within PSIS that serves as HRD's internal control. OMA plans to fully implement this control by April 30, 2020.

Closure of this recommendation will occur when PBGC provides evidence of the completed weekly and monthly quality checks.

Finding 2: PBGC Needs to Improve the COR Oversight Function at Contractor-Operated Facilities

PBGC Directive PM 25-05, *Selection, Designation, Training, and Management of Contracting Officer's Representatives* (May 1, 2017), establishes that the COR is “the eyes and the ears” of the Contracting Officer and plays a critical role in effective contract management. PBGC Directive IM 05-09, *PBGC Privacy Program* (May 21, 2018), states that protecting PII is the responsibility of every PBGC employee and contractor when performing PBGC’s mission. This directive establishes a framework to support a strong, multi-faceted PBGC privacy program. The PBGC Director retains overall responsibility and accountability for privacy protections and ensures that privacy policies are developed and implemented to mitigate the risk to PBGC’s operations, assets, and the individuals it serves. Department directors and managers are responsible for promoting the PBGC privacy program within their departments. Every PBGC employee and contractor is responsible for protecting PII.

Risk Advisory and Day-to-Day COR Oversight

In September 2018, our office issued a Risk Advisory, *Data Protection Considerations for the Field Office Support Services Procurement* (PA-18-125/SR 2018-15), to provide management with considerations and interim observations from fieldwork on this project. That report highlighted some of our observations relating to different data protection risk cultures and practices in the three contractor-operated offices we visited.

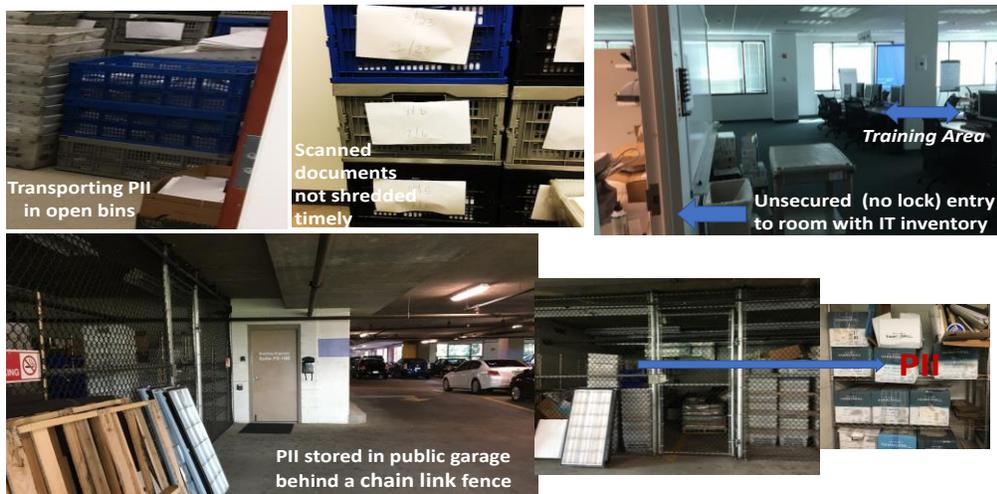
During fieldwork, we observed the following suitable practices at these offices:

- Locking scanned documents in a separate area (with only a few staff members having access to that area);
- Shredding of scanned documents in a timely manner;
- Manning the reception area during all working hours;
- Turning-off the fax machine outside of working hours;
- Restricting use of personal cell phones to scheduled breaks in non-working areas; and
- Maintaining a sign-in sheet in the server room.

We also identified data protection practices that need improvement (see Figure 3):

- Transporting scanned documents in open bins through unsecured space;
- Shredding of scanned documents in an untimely manner;
- Failing to lock an office containing IT inventory;
- Storing PII in a public garage behind a chain link fence; and
- Manning the reception area with gaps in coverage.

Figure 3: Data Protection Practices at Contractor-Operated Offices that Need Improvement



Source: OIG photos from site visits on Project No. PA-18-125 (taken July 27, 2018).

We noted that office cultures are driven by the tone set by top management, CORs and contractor Project Managers (PMs). Among the CORs and PMs at the three offices, we observed different levels of active engagement in day-to-day duties and awareness to situations that might result in the loss of sensitive information and an adverse effect on PGBC's reputation. We found some leadership behaviors that were not aligned with existing policies and procedures and did not promote urgency in protecting PII. The decreased engagement level and lack of vigilance may contribute to a permissive risk culture, resulting in increased risk of theft or accidental release of sensitive personal data.

Lack of Physical Access Restrictions

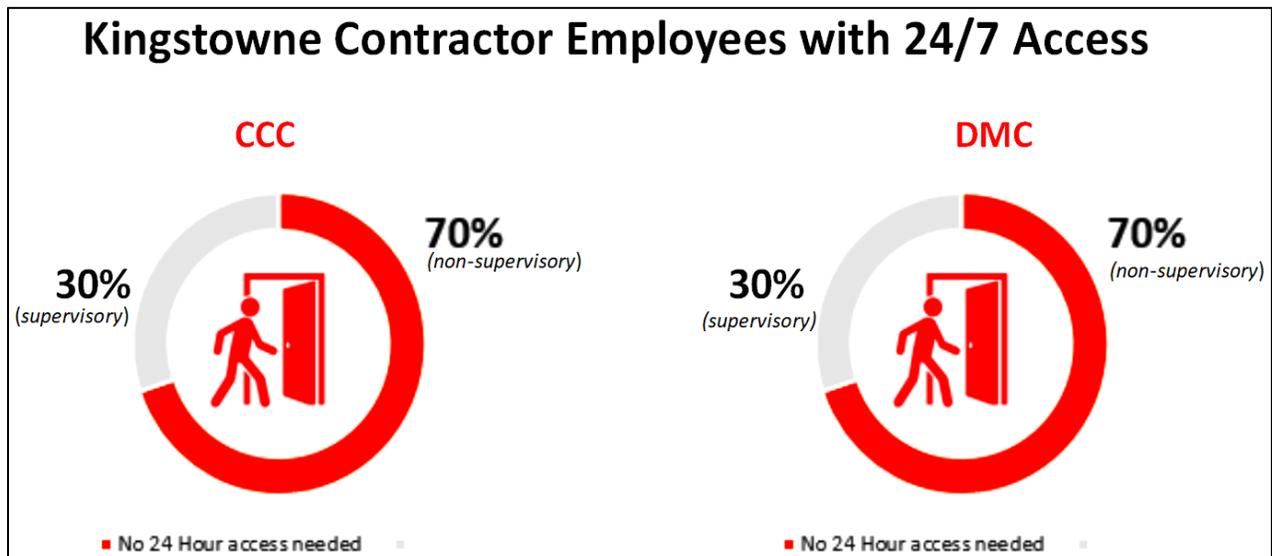
Directive IM 10-03, *Protecting Sensitive Information* (October 20, 2015), states that PBGC protects sensitive information by using physical safeguards such as key control management; and by limiting access within PBGC's offices to authorized individuals, including additional limitations based on the time of day, day of week, and the individual's official duties. One COR responsibility is to ensure that contractor employees are granted only necessary and appropriate physical access to the facilities. When completing Form 569, *Building and Security Access Request*, the COR indicates an access clearance level for an onboarding contractor employee, for example: 24/7 (unrestricted access) or 7:00 am to 7:00 pm (restricted based on the time of the day). Contractor employees use PBGC-issued PIV cards to access the authorized facilities. The regular working hours for the OBA's contractor-operated offices are Monday through Friday during the hours of 7:00 am to 7:00 pm.

We obtained physical access clearance listings for the three offices (Kingstowne, Miami, and Richmond Heights). Each office had a 24-hour access clearance listing for the local network

administrators or PBGC information technology personnel, a 24-hour access clearance listing for PBGC operations officials and contractor managers and supervisors, and restricted access clearance listings for all other contractor employees. In total, the three offices had 10 separate physical access clearance listings.

At the two contractor-operated facilities co-located at the Kingstowne location (the DMC and CCC), we found both centers allowed 24-hour access for all contractor employees working at this location, regardless of their management/supervisory status and official duties. See Figure 4.

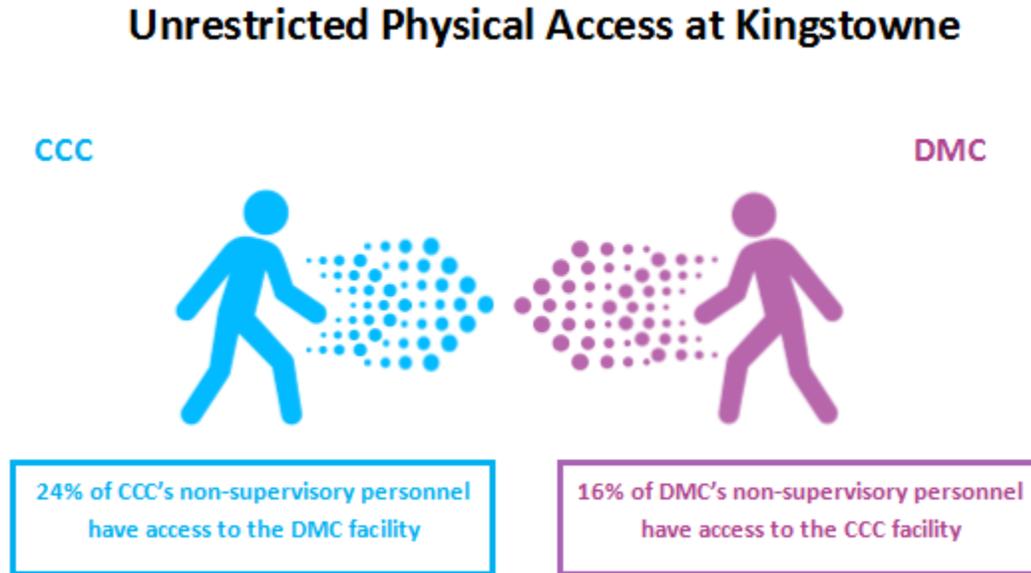
Figure 4. Kingstowne Contractor Employees with 24/7 Access facilities



Source: OIG Analysis of clearance access lists from PBGC.

The physical layout of the Kingstowne office exacerbates the risk of unauthorized physical access. The DMC and CCC are located on the same floor. They share the reception area in the middle. See Figure 5.

Figure 5. Unrestricted physical access at Kingstowne



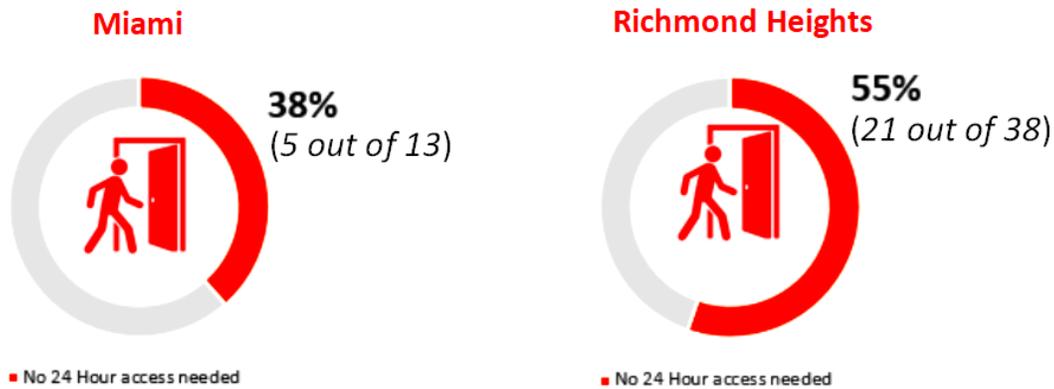
Source: OIG Analysis of clearance access lists from PBGC.

Although the two centers have some related business interactions usually done by supervisors for each center, the main scope of their work significantly differs. The DMC is the document management center and the CCC serves as the initial call center point of contact. During our visit to Kingstowne, PBGC officials and contractor management staff informed us that the employees of the DMC and CCC can access only their own areas. However, our review of the employee access clearance listings in the two facilities revealed that 24 percent of CCC's non-supervisory personnel have access to the DMC facility and 16 percent of DMC's non-supervisory personnel have access to the CCC office. In addition, we observed that the two centers share a lunch room which does not have PIV scanners, allowing anyone in the lunch area to enter either of the two facilities.

At the Richmond Heights and Miami offices we found numerous non-supervisory contractor employees who were granted 24-hour physical access clearances (see Figure 6). Local management acknowledged to the OIG that non-supervisors should not have 24-hour access.

Figure 6. Unrestricted Access at the Miami and Richmond Heights Facilities

Non-Supervisory Employees on Unrestricted Clearance Lists



Source: OIG analysis of clearance access lists from PBGC.

In addition, our analysis of the physical access clearance listings identified 36 separated employees in the 7 out of the 10 physical access clearance listings we reviewed.

In sum, physical access is not restricted in accordance with PBGC policy in the contractor-operated offices we visited. This was due to a lack of vigilance by CORs. This control failure increases the risk of leakage, theft, loss or unauthorized disclosure of sensitive participant data. Such events could potentially create benefit payment delays and inefficiencies and can lead to the loss of confidence and trust by stakeholders.

Recommendations

We recommend that the Office of Benefits Administration:

5. **Develop a process to ensure compliance with PBGC data protection policies and procedures at contractor-operated facilities, including the identified opportunities to improve physical security PII practices. (OIG Control Number OBA-4)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OBA stated they would develop a process to ensure compliance with PBGC data protection policies and procedures at contractor-operated facilities by October 31, 2019.

Closure of this recommendation will occur when PBGC provides evidence that OBA developed a process of ensuring compliance with PBGC data protection policies and

procedures at contractor-operated facilities.

- 6. Assess physical clearance access listings at contractor-operated offices based upon individual official duties and monitor physical access clearance listings as appropriate. (OIG Control Number OBA-5)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OBA stated that PSD would assess physical clearance access listings and monitor physical access clearance listings as appropriate. OBA, jointly with WSD, will identify and document positions with 24/7 access and restricted access (7:00 am to 7:00 pm) to the field sites, and apply those changes to all field locations to promote consistency. WSD Security will review the physical access of each field location contractor and make access level adjustments according to the agreed-upon positions and corresponding access levels. These changes can be implemented by April 1, 2019. Upon implementation WSD will provide continuous monitoring – for the first six months on a monthly basis and, after the first six months, a quarterly monitoring. OBA plans to complete these actions by October 31, 2019.

Closure of this recommendation will occur when PBGC provides evidence of the documented assessment of physical clearance access of field office positions, adjustments to access levels, and of monitoring access post revisions.

Finding 3: PBGC Needs to Improve Controls over Employee Separation Process

Controls relating to the separation process are critical to ensure that PBGC de-provisions or removes a separated individual's user access in a timely manner. The separation process for OBA contractor employees is a shared responsibility of many offices including OBA, the Information Technology Infrastructure Operations Department (ITIOD), and the Personnel and Physical Security team. According to the *Enterprise Systems and Services Separation SOP* (June 13, 2017) and the *Personnel Security SOP* (December 6, 2016), the Personnel Security team is responsible for updating personnel security records.

Employee Separation – System Access

According to the *Enterprise System and Services Separation SOP*, CORs are responsible for initiation of the separation process. Specifically, they are required to:

- Approve the contractor's separation request;

- Collect PBGC assets; and
- Facilitate the Enterprise Systems and Services separation process (a GetIT request).

We tested controls to determine if logical access to PBGC systems was disabled upon separation from employment at the contractor-operated facilities. We sampled 28 separated contractor employees who were either listed in PSIS as active or not found, as discussed above. We selected those employees to ensure the technical separation is complete. We determined that logical access for the sampled employees was ultimately disabled; however, not all CORs timely and accurately completed technical separation requirements. Specifically, the COR for Kingstowne's CCC did not submit separation requests for 5 out of the 22 contractor employees who separated during our review period. Those employees were eventually de-provisioned due to dormancy around 90 days (an IT established control) after the termination date. These accounts were only de-provisioned after five inactive account notices for each of the five separated contractor employees were sent to designated individuals (including the COR). The final inactive account notice is sent to the department director.

Both the PBGC *Cybersecurity and Privacy Catalog* and the *Enterprise System and Services Separation SOP* emphasize the timeliness of actions to be taken upon separation to prevent unauthorized access to PBGC information systems. Failure to timely de-provision system access can result in leakage, theft, loss or unauthorized disclosure of sensitive participant data. Such events could potentially create benefit payment delays and inefficiencies and can lead to the loss of confidence and trust by stakeholders.

Lack of Audit Trail

When a contractor employee separates from PBGC, the GetIT application will generate separation line items for fulfillment. For the Personnel and Physical Security team, GetIT creates four line items to fulfill as part of the separation process:

1. Update PSIS with effective separation date;
2. Disable physical access;
3. Terminate PIV card certificates; and
4. Collect and dispose separating individual's PIV card.

These line items are sent to the line item queue of the Personnel and Physical Security team. The team is responsible for reviewing its queues daily for any open line items. Each line item has mandatory fields that must be completed before a line item can be closed.

We evaluated 43 contractor employees from the Kingstowne CCC, Miami, and Richmond Heights offices who separated during the review period. We found that the Personnel and

Physical Security team did not consistently fulfill GetIT items and in some instances their actions lacked sufficient documentation.

For the first line item we found:

- 27 employees (or 63 percent) were not terminated in PSIS; and
- 1 employee had no record in PSIS.

For the remaining three-line items, we selected a sample of 9 out of the universe of 43 contractor employees (20 percent) to test whether these line items were completed timely and in accordance with the policies and procedures. According to the *Enterprise Systems and Services Separation* (Jun 13, 2017) SOP's fulfillment instructions, the Security team: collects any assets (e.g., PIV Card, Siemens or Datawatch fob) from separating employees, disables physical access to PBGC facilities in Siemens and/or Datawatch systems no later than the separation effective date, and terminates the separating employee's PIV card certificates in the General Services Administration (GSA) USAccess system within 5 business days of separation effective date. We found that in our sample of nine separated contractor employees:

- Physical access for all nine contractors was disabled in Siemens system; however, there was a record of *when* access was disabled for only one contractor employee.
- The PIV card credentials showed as terminated in the USAccess system for all contractors; however, the USAccess records did not have information on *when* credentials were terminated.
- We were not able to determine if the Security team received the PIV card for the nine contractors in our sample. PIV cards are received in various ways depending on location of the employee, and there is no required timeframe for collecting the PIV card. PBGC does not keep track of PIV cards received and disposed, nor do they have a defined process for collecting and tracking PIV card return.

The lack of documentation for separated contractor employees occurs because the Security team does not have a system in place to ensure the related action is completed after a GetIT ticket is generated. If PBGC cannot readily identify the status of separating employees, the agency is at risk should the separated employees gain unauthorized access to systems and facilities. In addition, if PIV cards are not tracked, the PBGC may not be aware of unauthorized use of the PIV card, such as displaying the card to gain access to other federal facilities.

The lack of an audit trail regarding separation, coupled with the lack of vigilant and consistent COR oversight, exacerbates the risk of unauthorized individuals accessing sensitive participant data and causing harm.

Recommendations

We recommend that the Office of Management and Administration:

- 7. Develop a process ensuring CORs are completing separation requests through GetIT in a timely manner, as required. (OIG Control Number OMA-6)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation. OMA stated that HRD is updating performance plans to ensure CORs process separations in GetITAll within two business days. In addition, HRD has coordinated with the Procurement Department to add language within COR designation letters outlining that all separation and transfer actions must be completed in GetITAll and within requisite timeframes. OMA's goal is to complete these actions by June 30, 2019.

Closure of this recommendation will occur when PBGC provides evidence that updated performance plans and revised language in the COR designation letter to ensure CORs are completing separation requests through GetIT in a timely manner have been implemented.

- 8. Develop a tracking mechanism to ensure GetIT requirements are fulfilled for separated employees. (OIG Control Number OMA-7)**

PBGC's Response and OIG's Evaluation

Resolved. PBGC concurred with the recommendation and stated that *Service Manager* is the tracking system of record and that a report may be requested from ITIOD of all corresponding line items along with line item completion dates, as necessary. OMA will use this report as a monitoring tool. OMA's goal is to complete this action by June 30, 2019.

Closure of this recommendation will occur when PBGC provides evidence that *Service Manager* provides the tracking of GetIT requirements under HRD's purview and that HRD is monitoring to ensure GetIT requirements are fulfilled for separated employees.

Other Matters

As noted above, our office issued a Risk Advisory in September 2018 on *Data Protection Considerations for the Field Office Support Services Procurement* (PA-18-125/SR 2018-15). That report was issued to provide management with some considerations and interim observations in light of PBGC's July 2018 issuance of a pre-solicitation, *Request for Information for Field Office Support Services*, to consolidate existing contractor-managed facilities and issue a single-award, multi-year indefinite delivery/indefinite quantity (IDIQ) contract. We observed that inconsistent data protection risk cultures and practices at contractor-managed facilities may subject PBGC and participants to increased risk of theft or accidental release of sensitive data. To mitigate these risks, we suggested that management strengthen contract language in the upcoming procurement, with enforceable terms, provisions, and metrics requiring safeguards for sensitive participant data.

We note that management has already taken a number of corrective actions in response to the Risk Advisory, to include adding new language in the Request for Procurement. Other corrective actions are underway. These actions are a step in the right direction, even if additional efforts as recommended in this report are needed to ensure the appropriate protection of sensitive participant data.

Appendix I: Objective, Scope, and Methodology

Objective

Our objective was to determine whether controls relating to data protection are suitably designed and operating effectively at contractor-operated facilities.

Scope

Our scope was limited to, and fieldwork was conducted at, the following locations:

- PBGC Headquarters, 1200 K St NW, Washington, DC 20005;
- Kingstowne CCC and DMC, 971 Kingstowne Village Pkwy, Alexandria, VA 22309;
- Miami FBA, 3750 NW 87th Ave, Miami, FL 33178; and
- Richmond Heights PVA, 26301 Curtiss Wright Pkwy #410, Cleveland, OH 44143.

We performed fieldwork from May through October 2018.

Methodology

To answer our objective, we reviewed the PBGC guidance: Directives PM 05-17, *Personnel Security and Suitability Program* (August 30, 2018); IM 10-03, *Protecting Sensitive Information* (October 30, 2015), IM 15-03, *PBGC Records Management Program* (August 17, 2015); *Cybersecurity and Privacy Catalog*, Version 1.2, of September 2017; and the standard operating procedures in *Personnel Security* (December 6, 2016) and *Enterprise Systems and Services Separation* (June 13, 2017). We also obtained access to the Personnel Security Investigation Solution (PSIS) used for capturing personnel security processing information. Finally, we performed observations at the contractor-operated facilities and interviewed contractor employees responsible for performing benefit administration duties. We interviewed personnel responsible for the management and oversight of benefit operations at the three field offices, as well as PBGC staff responsible for employee vetting and separation.

To evaluate PBGC compliance with policies and procedures for vetting contractor employees, we obtained employee listings from the Contracting Officer's Representatives and the security staff. We selected the universe of 65 contractor employees who onboarded the three sites during the period of November 2017 through April 2018 as those employees were captured in PSIS (the new personnel security processing application launched in November 2017). For evaluation of compliance for physical separation of contractor employees, we used the obtained employee listings and selected the universe of 43 contractor employees who

separated from the three sites during the period of November 2017 through June 2018. Out of the 43 contractor employees we selected a sample of 9 contractor employees (20 percent) to test whether these line items were completed timely and in accordance with the policies and procedures. In addition, we sampled 28 separated employees from the 43-employee universe to determine if access to PBGC systems was disabled upon separation from employment at the contractor-operated facilities.

Furthermore, we analyzed physical access clearances for the three locations to determine whether limitations are in place in the clearances to control access to facilities based on the time of day, day of week, and the individual's official duties.

Standards Followed During Evaluation Performance

We conducted the review under the authority of the Inspector General Act of 1978, as amended, and in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: Agency Response



Pension Benefit Guaranty Corporation

1200 K Street, N.W., Washington D.C. 20005-4026

To: Brooke Holmes
Assistant Inspector General for Audits

From: Alice Maroni *Alice Maroni*
Chief Management Officer

David Foley *David Foley*
Chief of Office of Benefits and Administration

Subject: Response to Office of Inspector General (OIG) Draft Evaluation Report,
Project No. PA-18-125

Thank you for the opportunity to comment on the OIG's draft evaluation report, dated December 20, 2018, relating to PBGC's Data Protection at Contractor-Operated Facilities. Your work on this is sincerely appreciated.

It was helpful to receive the associated Evaluation Results ahead of this report. This allowed for expeditious initiation of planning and remediation activities, which will lead to mutually desirable outcomes for the agency and the OIG.

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

Draft Evaluation Report, Project No. PA-18-125
PBGC's Data Protection at Contractor-Operated Facilities

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

Finding 1: PBGC Needs to Improve Monitoring and Management Oversight of the Personnel Security Process

Recommendation 1: Evaluate the effectiveness of the current Personnel Security Investigation Solution system and enhance the system functionality as necessary to ensure compliance with the PBGC policies.

PBGC Response: Management Concur.

The Personnel Security Investigation Solution system (PSIS) was introduced into production November of 2017. PSIS is a system for end to end tracking of background investigations, information and case files. The system collects information from multiple systems such as, GSA USAccess, FPPS, Active Directory, and OPM's eDelivery, to build person records within PSIS as well as manual inputs. Prior to deployment, PSIS ingested information from the Workplace Solutions Department's legacy system, PI Manager. The information contained within PI Manager was found to be outdated, incorrect and inconsistent. Nevertheless, due to timeliness, we migrated the data as we needed a baseline to work from.

As with all systems, enhancements were needed to include, unlocking data fields in order to update fields with true dates, adding a dashboard to better track workload and workflow, adding a position transfer dashboard, and migrating additional information into PSIS to build more comprehensive records. Since the enhancements has been made to PSIS, Personnel Security has been working diligently to update the records with accurate information and ensure records are in the correct workflow status. Since the enhancements have been made Personnel Security has been focusing on FY19 data and correcting identified anomalies.

This is a stand-alone system that does not impact other systems. No exports or outbound feeds come from PSIS which would have a compounding effect on OPM's Electronic Questionnaire for Investigative Processing e-QIP system or other databases.

The priority for Personnel Security in FY19 is to ensure all data within PSIS is complete and will continue to look for efficiencies to enhance the system.

Scheduled Completion Date: March 31, 2021.

Recommendation 2: Evaluate the existing employee vetting and security policies to ensure the policies and procedures reflect realistic deadlines.

PBGC Response: Management Concur.

There are several conditions that must be met in order for current policies and procedures to be effective. Personnel Security has two different elements to background investigations: 1. Prescreening and 2. Background Investigation.

HRD is in the process of updating internal Standard Operating Procedures (SOPs) to properly align with actual completion of timeframes.

We have also implemented steps if a new hire does not complete the background investigation questionnaire, Personnel Security will send 3 reminders to the applicant via email, contact the supervisor/Contracting Officers Representative (COR) of the employee/contractor to help inform the employee/contractor to complete the e-QIP process. If it is an employee, Personnel Security will reach out to the Human Resources Department's Employee and Labor Relations Management Division to assist. If it is a contractor, we will have the COR remove the contractor for failure to comply with PBGC Directive PM 05-17.

Scheduled Completion Date: September 30, 2019.

Recommendation 3: Develop and deliver training for personnel using Personnel Security Investigation Solution application to enhance understanding of the existing policy and requirements.

PBGC Response: Management Concur.

PSIS training sessions have been informally delivered to the Personnel Security team by Industrial Security Specialist, John Goldsby. The training sessions take place in one-on-one and group formats. The training sessions cover various topics, such as how to create person records, how to create a candidate record, how to update information, how information links to person/candidate records, etc. Updated PSIS user guides have also been distributed to the Personnel Security Team as a reference document. We are also contacting the vendor to conduct formal training sessions for staff as well.

Scheduled Completion Date: April 30, 2019

Recommendation 4: Develop a control to ensure PSIS information is complete, accurate and timely.

PBGC Response: Management Concur.

HRD has established weekly and monthly quality checks of new person information within PSIS that serves as HRD's Internal Control.

Scheduled Completion Date: April 30, 2020

Finding 2: PBGC Needs to Improve the COR Oversight Function at Contractor-Operated Facilities

Recommendation 5: Develop a process to ensure compliance with PBGC data protection policies and procedures at contractor-operated facilities, including the identified opportunities to improve physical security PII practices.

PBGC Response: Management Concur.

OBA/PSD will develop a process to ensure compliance with PBGC data protection policies and procedures at contractor-operated facilities.

Scheduled Completion Date: 10/31/2019

Recommendation 6: Assess physical clearance access listings at contractor-operated offices based upon individual official duties and monitor physical access clearance listings as appropriate.

PBGC Response: Management Concur.

- PSD will assess physical clearance access listings and monitor physical access clearance listings as appropriate.
- WSD will partner with OBA to identify and document which positions should have 24/7 access and restricted access (7 am to 7 pm) access to the field sites. These changes will be applied to all field locations as they all have the same positions, thus promoting consistency.
- WSD Security will review the physical access of each field location contractor and make access level adjustments according to the agreed upon positions and corresponding access levels. These changes can be implemented by April 1, 2019.
- Continuous Monitoring: Once monthly, for the first six months following implementation, WSD will complete a reconciliation of all field location contractor access levels to ensure each contractor has the appropriate level. WSD will coordinate with the OBA CORs where necessary to clarify any changes. After the first six months of monthly monitoring, WSD will conduct quarterly monitoring of the field location physical access levels for all corresponding contractors.

Scheduled Completion Date: 10/31/2019

Finding 3: PBGC Needs to Improve Controls over Employee Separation Process

Recommendation 7: Develop a process ensuring CORs are completing separation requests through GetIT in a timely manner, as required.

PBGC Response: Management Concur.

HRD is updating performance plans to ensure CORs process separations in GetITAll within 2-business days. Furthermore, HRD has coordinated with the Procurement Department to add language within COR designation letters outlining that all separation and transfer actions must be completed in GetITAll and within requisite timeframes.

An example of the language to be used within performance plans is as follows:

- Adheres to onboarding procedures within personnel security prescribed deadlines. Upon entrance, ensures contractor employees receive least privileged access and if responsibilities change, appropriate access levels are readjusted within the established timeframes.
- Submits the COR checklist in accordance with the established process. Checklist and required documentation must be complete, accurate and legible.
- Before contractor departure or within 2-business days of contractor departure notifies appropriate offices to ensure exiting contractor access to information systems, property, and facilities are revoked. Submits:
 - PIV access card
 - GET IT request for exiting and all other PBGC access forms
- COR will attend Personnel Security hosted training for CORs

Scheduled Completion Date: June 30, 2019.

Recommendation 8: Develop a tracking mechanism to ensure GetIT requirements are fulfilled for separated employees.

PBGC Response: Management Concur.

HRD is a recipient of line items from ITIOD's system Service Manager. The line items are generated from requests through GetITAll. Once HRD receives a line item, we take appropriate actions to complete the related line items. Line item completion is tracked through Service Manager. Service Manager also serves as the system of record and is considered the tracking mechanism. A report may be requested from ITIOD of all corresponding line items along with line item completion dates, as necessary.

Scheduled Completion Date: June 30, 2019

Appendix III: Acronyms

CCC	Customer Contact Center
COR	Contracting Officer's Representative
e-QIP	Electronic Questionnaires for Investigations Processing
FBA	Field Benefit Administrator
HRD	Human Resources Department
PII	Personally Identifiable Information
OIG	Office of the Inspector General
OBA	Office of Benefits Administration
OMA	Office of Management and Administration
PBGC	Pension Benefit Guaranty Corporation
PIV	Personal Identification Verification
PSIS	Personnel Security Investigation Solution

Appendix IV: Staff Acknowledgements

Staff Acknowledgement

Parvina Shamsieva-Cohen, Audit Manager; Christina Harris Auditor-In-Charge; and Natali Dethomas, Auditor, made key contributions to this report.

Appendix V: 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
1200 K Street, NW, Suite 480
Washington, DC 20005

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.