September 11, 2018

RISK ADVISORY

TO: David Foley
Chief of Benefits Administration

Judith Starr
General Counsel

Alice Maroni
Chief Management Officer

FROM: Robert A. Westbrooks *Robert A. Westbrooks*
Inspector General

SUBJECT: Data Protection Considerations for the Field Office Support Services Procurement (PA-18-125/SR 2018-15)

As you know, our office is conducting an evaluation of data protection at contractor-managed facilities to ensure sensitive participant data is appropriately safeguarded (Project No. PA-18-125). We expect to issue a final report in the coming months. We are issuing this Risk Advisory 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*. We understand PBGC intends to consolidate existing contractor-managed facilities and issue a single-award, multi-year indefinite delivery/indefinite quantity (IDIQ) contract in March 2019.

The suggestions contained in this Risk Advisory do not constitute formal audit recommendations; therefore, no management response is required. If management does take action because of this Risk Advisory, we respectfully request a written summary of the action taken. Please be advised, we will post this Risk Advisory on our public website in accordance with our responsibilities under the Inspector General Act to keep the Board, Congress, and the public fully and currently informed about problems and deficiencies related to the Corporation's programs and operations.

Summary

As you know, management is responsible for identifying internal and external risks that may prevent the Corporation from meeting its strategic goals and objectives, assessing risks to

determine their potential impact, and applying the appropriate risk responses. One source of risk information is the OIG. During the course of our data protection evaluation, we observed risks that warrant management's attention. Specifically, we observed different data protection risk cultures and practices in the contractor-managed offices we visited. Such variations from office-to-office reflect unintended flexibility in current contracts which can contribute to a permissive risk culture and subject PBGC and participants to increased risk of theft or accidental release of sensitive personal data. To better safeguard participant data and mitigate the risk of loss, we suggest management promote a more uniform data protection risk culture by strengthening contract language in the pending Field Office Support Services procurement. Involvement of the Corporation's Privacy Officer is paramount in ensuring enforceable and privacy compliant contract language.

Background

OBA manages the termination process for defined benefit plans, provides participant services (including calculation and payment of benefits) for PBGC trusteed plans, provides actuarial support for PBGC, and carries out PBGC's responsibilities under settlement agreements.

Currently, contractor-managed facilities across the country perform benefit administration duties for approximately 1.4 million participants. The Field Benefits Administration (FBA) offices in Coraopolis, PA; Miami, FL; Sarasota, FL; and Wilmington, DE are focused on processing the active inventory of approximately 500 plans. The Post Valuation Administration (PVA) field office in Richmond Heights, OH administers over 4,000 post valuation plans. The Customer Contact Center (CCC) serves as the initial contact point for participants, and the Document Management Center (DMC) provides document and records management. Both centers are located in Kingstowne, VA.

Risk

With the planned consolidation of services, 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.

Details

Enterprise Risk Management

Office of Management and Budget Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* requires PBGC to maintain an effective risk

management program that identifies, assesses, and responds to risks related to mission delivery (such as pension benefits administration). Risks must be analyzed in relation to the achievement of strategic, operational, reporting, and compliance objectives (such as adherence to laws, policies, rules, and regulations relating to the protection of sensitive data). Circular A-123 also notes that agencies may find it useful to consider the concept of reputational risk, or the loss of confidence and trust by stakeholders. Effective risk management response to emerging risks takes human and cultural factors into account, considers qualitative and quantitative information, and facilitates continual improvement of the organization.

Both PBGC and our office have identified data loss and contactor oversight as major risks facing the Corporation. In the past few years, our office has worked constructively with the PBGC Privacy Officer, the Chief Information Security Officer, the Chief of Benefits Administration, and others to address these shared concerns.

Data Protection/Privacy Risk Culture

As stated in Circular A-123, "to complete this circle of risk management the Agencies must incorporate risk awareness into the agencies' culture and ways of doing business." According to the CEB (now known as Gartner) Risk Management Leadership Council, organizations can build a risk aware culture through training, embedding risk aware behaviors in ongoing business processes, and communicating continuously.[1] Gartner identifies a number of metrics used by organizations to measure patterns in risk management behaviors; these metrics include, for example: recorded instances of policy non-compliance, training completion rates, percentage of issues self-identified by the business, percentage of issues identified within X days of risk event, and number of staff members disciplined or terminated for related misconduct.[2] Further, in its research and analysis, Gartner identifies "cultural permissiveness" as among the most common causes of data privacy risk events.[3]

Under PBGC Directive IM 05-09, *PBGC Privacy Program* (May 21, 2018), protecting personally identifiable information (PII) is an integral part of PBGC's business operations and must be a core consideration for every PBGC department, employee, and contractor. The 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. In addition, all PBGC Department Directors and Managers

[1] CEB Risk Management Leadership Council, *Reinforce a Risk-Aware Culture*, Member Hosted Forum, New York, NY (April 10, 2014).
[2] Gartner Risk Management Leadership Council, *Measuring and Influencing Risk Climate*, White Paper (2018).
[3] Gartner Risk Management Leadership Council, *Primer for Data Privacy Risk Management*, Tool (January 24, 2018).

are responsible for promoting the PBGC privacy program within their departments, and protecting PII is the responsibility of every PBGC employee and contractor. The updated directive underscores a shared responsibility for protecting PII.

OIG Observations

As a part of our data protection project, we conducted interviews and observations at three contractor-managed locations: the CCC and DMC offices in Kingstowne, VA; the FBA office in Doral, FL; and the PVA in Richmond Heights, OH. We observed different data protection cultures and practices in these contractor-managed offices, as described below.

Data protection risk cultures: We observed office cultures are driven by the tone set by top management, Contracting Officer representatives (CORs) and Project Managers (PMs). In some offices, consistent, visible management leadership promoted a culture of data protection. For example, posting the most recent "Help Prevent Fraud at PBGC" e-mail throughout one office site increased employee awareness about potential fraud and data protection. Project Managers and CORs also promoted PBGC's data protection culture by conducting office walkthroughs (including surprise walkthroughs) that prompted compliance with internal practices to protect PII data when employees are not at their desks.

Among the CORs and PMs, 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 adverse effect on PGBC's reputation. Some leadership behaviors are not aligned with existing policies and procedures and do not promote urgency in protecting PII. At one site, for example, a staff member relayed, when they moved through the office assisting others, PII was not secured in workspaces as required. Additional examples are included in office practices below. This 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.

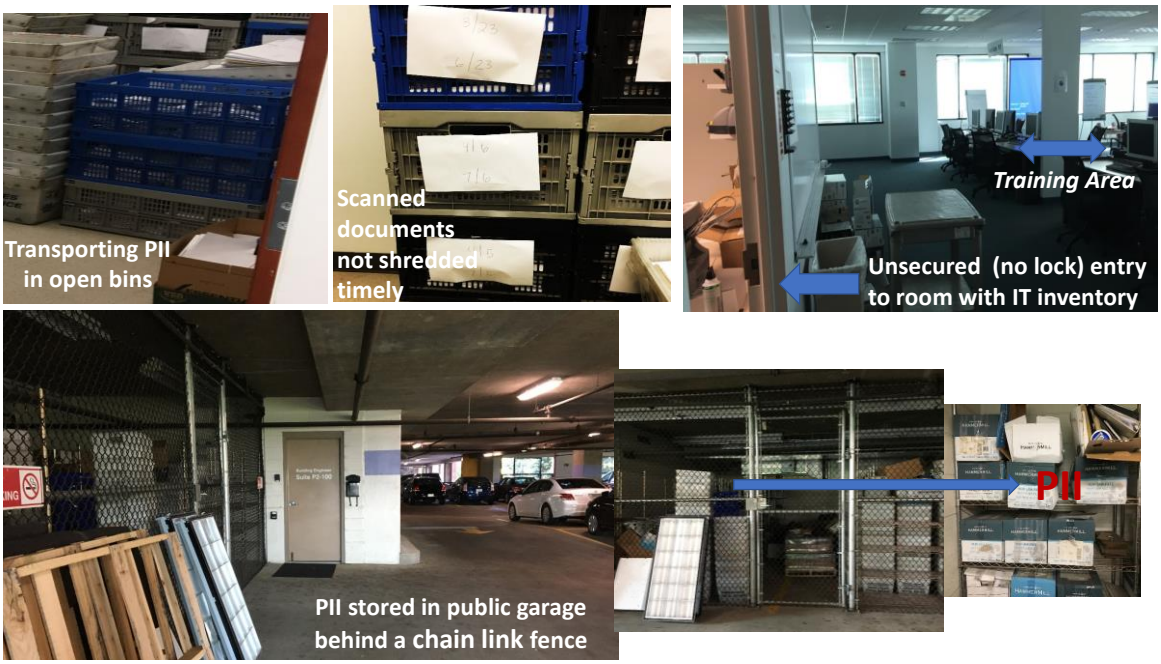
Office practices. While all of the offices cited PBGC policies and procedures for their day-to-day operations, we observed practices for protecting PII varied among offices. At some locations, we observed the following suitable practices:

- 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.

At other locations, we identified data protection practices that need improvement (see Figure 1):

- 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 1: Opportunities to Improve PII Practices



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

In addition, we noted the absence of cameras at entry and exit doors, varying ability to use personal cell phones at work stations, and inconsistent practices with visitor access.

Conclusion

Under Circular A-123 and PBGC Directive IM 05-09, protecting PII is an integral part of PBGC's business operations and must be a core consideration for every PBGC contractor. However, CORs and PMs, in some contractor offices, were not fully engaged in creating an awareness among employees to vigilantly protect sensitive data. Also, some contractor offices have

opportunities to improve their PII practices. These shortcomings increase PBGC and participant risk for theft or accidental release of PII.

Strengthening accountability and creating the desired data protection risk culture, at all levels, requires defining and standardizing critical measures. Although PBGC has policies and procedures pertaining to data protection in place, firmly embedding and integrating the desired privacy practices within the planned field office support services procurement is essential.

The Corporation may want to consider more explicit contract terms governing training, security, program management, performance requirements, and quality assurance. Management should additionally consider enforcement of requirements to secure participant plan documents in locked areas, maintenance of security cameras, facility access restrictions, and adherence to scanned document disposal schedules.

Suggestions

To mitigate the above risks, we offer the following suggestions:

The Office of Benefits Administration, in conjunction with the Procurement Department, should consider reinforcing PBGC's data protection/privacy risk culture by strengthening contract language in the upcoming procurement. The contract should have enforceable terms, provisions and metrics requiring safeguards for sensitive participant data.

The Corporation's Privacy Officer should participant in this procurement to help ensure enforceable and privacy compliant contract language is considered.

cc: Marty Boehm, Director, CCRD
Jennifer Messina, Director, PSD
Roland Thomas, Acting Director, PD
Margaret Drake, Chief Privacy Officer
Nicole Puri, Risk Management Officer
Phil Hertz, Senior Agency Official for Privacy