



governmentattic.org

"Rummaging in the government's attic"

Description of document: Five (5) Pension Benefit Guaranty Corporation (PBGC) Inspector General (OIG) Management Advisory Reports 2017-2020 and list of PBGC OIG Risk Advisory and Management Advisory Reports 2012-2020

Requested date: 23-February-2020

Release date: 09-July-2020

Posted date: 10-August-2020

Source of document: FOIA Request
Disclosure Officer
Pension Benefit Guaranty Corporation
1200 K Street, N.W., Suite 11101
Washington, D.C. 20005
Phone: (202) 229-4040
Fax: (202) 229-4042
[FOIAonline](#)

The governmentattic.org web site ("the site") is a First Amendment free speech web site, and is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



Pension Benefit Guaranty Corporation
1200 K Street, N.W., Washington, D.C. 20005-4026

BY EMAIL

PBGC 2019-001848

July 9, 2020

RE: Request for Management Advisory Reports

I am responding to your request, dated February 23, 2020, and received by the Disclosure Division of the Pension Benefit Guaranty Corporation (PBGC) March 27, 2020. You requested a copy of the following: (1) Management Advisory, Management Advisory Memorandum, and Management Advisory Report produced by the PBGC Office of Inspector General (OIG) since January 1, 2017; and a (2) printout of the listing of Management Advisories, Management Advisory Memoranda, and Management Advisory Reports issued by PBGC's OIG since January 1, 2010. You authorized fees in the amount of \$25.00. We processed your request in accordance with the Freedom of Information Act (FOIA) and PBGC's implementing regulation. Please accept my apology for the delay.

Pursuant to your request, the OIG conducted a search of their records. They located 40 pages responsive to Items 1 and 2 of your request. I have determined that 17 pages may be released to you in full, as described below:

Item 1 (16 pages):

- Risk Advisory - Additional Measures to Address Fraud Vulnerabilities in Benefits Administration (SR-2020-07) (Public Version), dated January 21, 2020 (1 page);
- Risk Advisory - Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats (SR-2019-09/RA-19-001) (Public Version), dated March 8, 2019 (2 pages);
- Risk Advisory - Data Protection Considerations for the Field Office Support Services Procurement (PA-18-125/SR 2018-15), dated September 11, 2018 (6 pages);
- Risk Advisory - MyPBA Web Application Control Weaknesses (PA-16-115/RA-2018-03), dated November 15, 2017 (5 pages); and
- Summary of Actions Taken on Risk Advisory - My PBA Web Application Control Weaknesses, dated October 19, 2018 (2 pages).

Item 2 (1 page):

- List of PBGC OIG's Risk Advisory and Management Advisory Reports since 2010 (1 page).

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA, *See* 5 U.S.C. 552(c) (2019). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all requesters and should not be taken as an indication that excluded records do, or do not exist.

It was necessary to withhold 23 pages entirely, consisting of inter/intra-agency memoranda. The PBGC reasonably foresees that disclosure of this information would harm interests protected by the FOIA. I have relied on three FOIA exemptions to withhold this information.

The first applicable FOIA exemption, 5 U.S.C. § 552(b)(5), deals with internal documents: inter-agency or intra-agency memoranda or letters consisting of judgments, opinions, advice or recommendations which would not be available by law to a party other than an agency in litigation with PBGC and as such are not required to be disclosed under 5 U.S.C. § 552(b)(5). This exemption also protects from disclosure attorney client communications and the agency's deliberative processes. I have determined that the disclosure of this material would not further the public interest at this time and would impede the operations of PBGC.

The second applicable exemption, 5 U.S.C. § 552(b)(6), exempts from required public disclosure, "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy." Some of the records you have requested contain "similar files" within the meaning of the above cited statutory language and PBGC's implementing regulation (29 C.F.R. § 4901.21(b)(4)). In applying Exemption 6, a balancing test was conducted, weighing the privacy interests of the individuals named in the document against the public interest in disclosure of the information. The public interest in disclosure is one that "sheds light on an agency's performance of its statutory duties." *Dep't of Justice v. Reporters Committee*, 489 U.S. 749, 773 (1989). I have determined disclosure of this information would constitute a clearly unwarranted invasion of personal privacy.

Finally, the third applicable FOIA exemption, 5 U.S.C. § 552(b)(7)(E), permits the exemption from disclosure of "records or information compiled for law enforcement purposes . . . [that] would disclose techniques and procedures for law enforcement investigations or prosecutions." Accordingly, § 552(b)(7)(E), protects records or information that could interfere with enforcement proceedings and disclose techniques and procedures for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. Some of the records responsive to your request contain information which falls within the meaning of the above-cited statutory language. I have determined disclosure of the information could reasonably create a risk of circumvention of the law.

Since this response constitutes a partial denial of records, I am providing you your administrative appeal rights in the event you wish to avail yourself of this process. The FOIA provides at 5 U.S.C. § 552(a)(6)(A)(i) (2014) amended by FOIA Improvement Act of 2016, Pub. L. No. 114-185, 130 Stat. 538 that if a disclosure request is denied in whole or in part by the Disclosure Officer, the requester may file a written appeal within 90 days from the date of the denial or, if later (in the case of a partial denial), 90 days from the date the requester receives the disclosed material. PBGC's FOIA regulation provides at 29 C.F.R. § 4901.15 (2017) that the appeal shall

state the grounds for appeal and any supporting statements or arguments, and shall be addressed to the General Counsel, Attention: Disclosure Division, Pension Benefit Guaranty Corporation, 1200 K Street, N.W., Washington, D.C. 20005. To expedite processing, the words "FOIA Appeal" should appear on the letter and prominently on the envelope.

In the alternative, you may contact the Disclosure Division's Public Liaison at 202-326-4040 for further assistance and to discuss any aspect of your request. You also have the option to contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about their FOIA mediation services. The contact information for OGIS is as follows: Office of Government Information Services, National Archives and Records Administration, 8601 Adelphi Road-OGIS, College Park, Maryland 20740-6001; e-mail at ogis@nara.gov; telephone at 202-741-5770; toll free at 1-877-684-6448; or facsimile at 202-741-5769.

This completes our processing of your request. Your request was categorized as "Other." Under this category, requesters are subject to search and duplication costs.¹ Since processing costs were assessed below our nominal fee of \$25.00, I have not charged fees for processing this request.

You may submit future requests for PBGC records by accessing FOIAonline, our electronic FOIA processing system, at: <https://foiaonline.gov>, or by e-mail at Disclosure@pbgc.gov.

Sincerely,



D. Camilla Perry
Disclosure Officer
Office of General Counsel
General Law and Operation Department

Enclosures

¹ See 5 U.S.C. § 552(a)(4)(ii) (I).



January 21, 2020

RISK ADVISORY

TO: David Foley
Chief of Benefits Administration

Jennifer Messina
Director, Participant Services Department

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

SUBJECT: Additional Measures to Address Fraud Vulnerabilities in Benefits
Administration (SR-2020-07) (PUBLIC VERSION)

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.

Management is specifically responsible for identifying and managing its fraud risks. This includes designing and implementing control activities to prevent and detect fraud. As you know, in recent months we have observed an increase in fraudulent activity in benefits administration. We provided management with a non-public version of this Risk Advisory with our observations regarding certain fraud vulnerabilities and suggestions for PBGC management to consider to prevent additional losses to PBGC or participants.



Office of Inspector General
Pension Benefit Guaranty Corporation

March 8, 2019

RISK ADVISORY

TO: Tom Reeder
Director

Robert Scherer
Chief Information Officer

Judith Starr
General Counsel

David Foley
Chief of Benefits Administration

Alice Maroni
Chief Management Officer

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

SUBJECT: Additional Safeguards are Needed to Protect Sensitive Participant Data from
Insider Threats (SR-2019-09/RA-19-001) (PUBLIC VERSION)

We are issuing this Risk Advisory to urge management to consider additional safeguards to protect sensitive participant data from insider threats based on recent OIG findings and long-standing concerns.

As you know, following a compromise of personally identifiable information on or about January 2018, our office conducted a criminal investigation to identify the person(s) responsible. In addition to our investigative response, we initiated an evaluation of *PBGC's Data Protection at Contractor-Operated Facilities* to ensure sensitive participant data is appropriately safeguarded (EVAL-2019-08/PA 18-125). We completed our evaluation and reported our findings and recommendations on January 31, 2019. During that project, we issued a separate Risk Advisory on September 11, 2018, on *Data Protection Considerations for the Field Office Support Services Procurement* (SR-2018-15). Please be advised that the criminal investigation is now concluding as well. We will notify management and report the outcome of the criminal investigation when the case is resolved in federal court.

We are providing management with a separate non-public version of this Risk Advisory to share the details regarding these additional safeguards. The suggestions contained in the restricted information Risk Advisory do not constitute formal audit recommendations; therefore, no

written management response is required. We will post this public version Risk Advisory on our 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.

cc: Frank Pace, Acting Director, CCRD
Latreece Wade, Acting RMO
Tim Hurr, CISO
Margaret Drake, Chief Privacy Officer
Phil Hertz, Senior Agency Official for Privacy



Office of Inspector General
Pension Benefit Guaranty Corporation

September 11, 2018

RISK ADVISORY

TO: David Foley Judith Starr
Chief of Benefits Administration 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 trustee 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 PBGC’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.

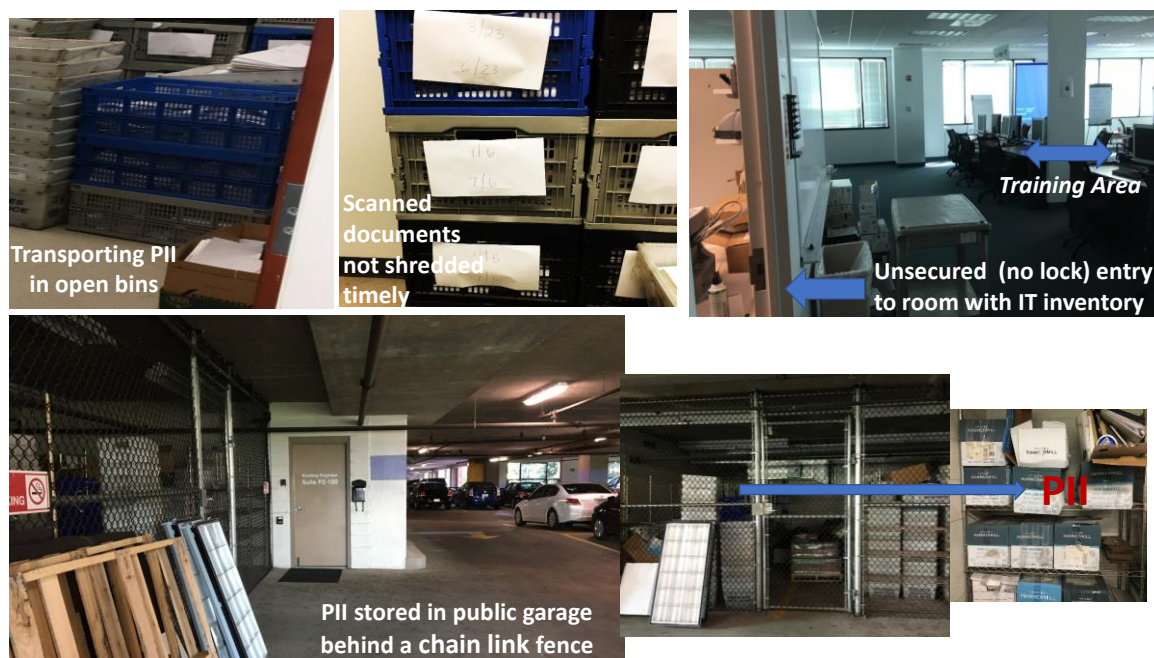
Office practices. While all of the offices cited PBGC policies and procedures for their day-to-day operations, we observed practices for protecting PII varied among offices. At some locations, we observed the following suitable practices:

- 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 participate 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



Office of Inspector General Pension Benefit Guaranty Corporation

November 15, 2017

RISK ADVISORY


To: Tom Reeder
Director

Bob Scherer
Chief Information Officer

Cathy Kronopolus
Chief of Benefits Administration

Tim Hurr
Chief Information Security Officer

Nicole Puri
Risk Management Officer

From: Robert A. Westbrooks
Inspector General 

Subject: MyPBA Web Application Control Weaknesses (PA-16-115) / RA-2018-03

This Risk Advisory is to report our concerns regarding control weaknesses within the MyPBA web application. 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. We previously provided management with detailed information regarding the controls in question and our observations. The detailed information is not repeated in this public report due to its sensitive nature.

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. We have identified the following risks that warrant management's

attention: (1) the MyPBA application operates without certain PBGC-standard access controls and identification and authentication controls, and (2) the MyPBA application does not utilize multi-factor authentication to help protect the security of sensitive data and online transactions.

To mitigate these risks to an acceptable level, we suggest (1) the Office of Benefits Administration (OBA) develop a plan of action and milestone (POA&M) to address and track the control deficiencies; and (2) the Enterprise Cybersecurity Division (ECD) review the applicable guidance on multi-factor authentication, consider the practices of other federal agencies including Social Security Administration (SSA), and confer with OBA on the MyPBA application to ensure that the consideration of multi-factor authentication is documented as part of the next MyPBA upgrade requirements analysis.

Background

MyPBA is a web-based application intended to reduce the call volume to the PBGC's Customer Contact Center. MyPBA has over 131,000 active accounts, and participants completed 747,701 transactions in FY 2017. Participants applying for an account are required to provide: first name, last name, social security number, and PBGC plan name or plan number.

MyPBA enables individual participants to obtain plan-specific and benefit-specific information from PBGC; allows participants to make web-based benefit inquiries with PBGC through secure web-based channels; and allows participants to conduct web-based benefit-related transactions including change payment method, claim a beneficiary, and apply for pension benefits.

Risks

- *The MyPBA application operates without certain PBGC-standard access controls and identification and authentication controls, and*
- *The MyPBA application does not utilize multi-factor authentication to help protect the security of sensitive data and online transactions.*

Details

Responsibilities

Under PBGC Directive IM 05-02, *PBGC Information Security Policy*, the PBGC Director has overall responsibility and accountability for information security protections commensurate with the risk and impact of harm to the PBGC's operations, assets, and individuals within the organization; and for ensuring development and implementation of policies to establish PBGC's commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions performed by PBGC. The Chief Information Officer is responsible for providing advice and other assistance to the PBGC Director and other senior officials to ensure that information technology is acquired and information resources are managed for the agency in a manner that is consistent with the Clinger-Cohen Act and FISMA; and for ensuring the development and implementation of policies to establish PBGC's commitment to information security and the actions required to effectively manage risk and protect the core missions and business functions performed by PBGC. The Chief Information Security Officer is responsible for developing, documenting, and implementing an agency-wide IT security program to provide information security for the information and information systems that support the operations and assets of the agency in the most cost-effective manner; for assisting senior PBGC officials in performing their information security responsibilities; and for reviewing and approving cybersecurity policy deviations where appropriate. Information system owners are responsible for maintaining overall accountability for the procurement, development, integration, modification, or operation and maintenance of an information system; and for ensuring compliance with information security requirements.

As part of its responsibilities to provide participant services for the calculation and payment of benefits for PBGC-trusted plans, OBA manages the MyPBA application and is the MyPBA information system owner. OBA released version 1.4.6 of MyPBA in July 2017 and plans to release version 1.4.7 in December 2017.

The MyPBA application operates without certain PBGC-standard access controls and identification and authentication controls.

The Federal Information Security Management Act (FISMA) assigns the responsibility for developing federal information security guidelines and standards to the National Institute of Standards and Technology (NIST). NIST guidance is published in various special publications (SP). SP 800-53, revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* establishes minimum standards for operating and controlling federal agencies IT systems.

The PBGC Cybersecurity and Privacy Catalog (CPC) documents PBGC's security and privacy policies and minimum control standards as required by FISMA and NIST standards, and provides

a common reference to be used by PBGC personnel. The CPC also establishes the minimal baseline requirements for each control but more stringent requirements can be enforced at the discretion of the system's Authorizing Official.

PBGC's Enterprise Cybersecurity Division conducts security assessments of PBGC systems. According to the March 2017 MyPBA Security Assessment Report, certain baseline controls have not been implemented. These controls relate to passwords, login, and inactive accounts. Current MyPBA password requirements meet NIST standards but do not meet the additional PBGC baseline requirements. OBA advised the OIG that these controls were not implemented due to the desire to balance customer service, convenience, and readiness. OBA performed a Business Impact Analysis in February 2017 and accepted the risks associated with these unimplemented controls. While the acceptance of risk is a management function, we believe management should have conducted additional analysis to include consideration of cost of controls and impact on participants.

The failure to implement these controls leaves the MyPBA web application vulnerable to intruder attacks and possibly theft of participant benefit payments, notwithstanding the presence of some compensating controls. We note that after we first communicated our concerns to OBA, management took steps to improve the password reset functionality. OBA has also reported to us that they plan to implement additional controls to bring MyPBA into compliance with PBGC policies.

The MyPBA Web Application does not utilize multi-factor authentication to help protect the security of sensitive data and online transactions.

While multi-factor authentication is not yet a required federal standard, it is a best practice and one that the White House has encouraged federal agencies to adopt to protect federal transactions online. In Executive Order 13681, *Improving the Security of Consumer Financial Transactions*, the President ordered the National Security Council staff, the Office of Science and Technology, and OMB to present a plan to ensure that all agencies making personal data accessible to citizens through digital applications require the use of multiple factors of authentication and an effective identity proofing process, as appropriate. The subsequent President's Cybersecurity National Action Plan calls for the utilization of multi-factor authentication to secure Americans' online accounts. While phase-in dates for multi-factor authentication have not been established, some agencies have already implemented this standard to better protect accounts from unauthorized use and potential identity fraud. For example, in June 2017 the Social Security Administration implemented multi-factor authentication within the mySocialSecurity (mySSA) application after the SSA Office of

Inspector General raised concerns about data security. In addition to a username and password, mySSA account holders are now able to choose either their cell phone or their email address as a second identification method.

OBA previously determined that the developmental expense of multi-factor authentication was too high for a non-mandatory requirement. We believe that PBGC cybersecurity standards should not be limited to mandatory, or minimal requirements, but should be based on the threat environment within MyPBA and comparable federal systems, the risk and impact of potential adverse effects to participants and PBGC, and the availability of cost-effective controls. Further, given the apparent inevitability of a multi-factor authentication requirement, management should consider a more proactive approach towards planning and implementation.

Suggestions

To reduce the risk of waste, fraud, and abuse, and to enhance program performance, we offer the following suggestions:

The Office of Benefits Administration should develop a POA&M to address and track the control deficiencies associated with the MyPBA web application.

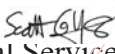
The Enterprise Cybersecurity Division should review the applicable guidance on multi-factor authentication, consider the practices of other federal agencies including SSA, and confer with OBA on the MyPBA application to ensure that the consideration of multi-factor authentication is documented as part of the next MyPBA upgrade requirements analysis.



Pension Benefit Guaranty Corporation
1200 K. Street, N.W., Washington, D.C. 20005-4026

October 19, 2018

To: Robert A. Westbrooks
Inspector General

From: Scott G. Young  Digitally signed by
SCOTT YOUNG
Date: 2018.10.19
17:44:10
Director, Actuarial Services and Technology Department (ASTD)

Subject: Summary of Action Taken in Response to
Risk Advisory - MyPBA Web Application Control Weaknesses

As requested, we have prepared this summary to update you on the actions taken in response to the Risk Advisory regarding MyPBA Web Application Control Weaknesses, dated November 15, 2017.

Risk: The MyPBA application operates without certain PBGC-standard access controls and identification and authentication controls

Suggestion: The Office of Benefits Administration should develop a POA&M to address and track the control deficiencies associated with the MyPBA web application.

Action Taken: MyPBA Release 1.4.9, deployed September 14, 2018, included the PBGC requirements as defined in the Cybersecurity and Privacy Catalog for access (AC) controls and identification and authentication (IA) controls regarding disabling accounts, invalid login attempts, and passwords. The release brings MyPBA into compliance with PBGC standards. This risk should be considered addressed along with the related suggestion to develop a PO&AM to address and track control deficiencies associated with the MyPBA web application.

Risk: The MyPBA application does not utilize multi-factor authentication to help protect the security of sensitive data and online transactions

Suggestion: The Enterprise Cybersecurity Division should review the applicable guidance on multifactor authentication, consider the practices of other federal agencies including SSA, and confer with OBA on the MyPBA application to ensure that the consideration of multi-factor authentication is documented as part of the next MyPBA upgrade requirements analysis.

Action Taken: Over the next few years, OBA plans to modernize the MyPBA system. We recently completed an alternatives analysis project that conducted market research on various commercial customer experience options for consideration. Multi-factor authentication is

documented as a requirement for future development. In addition, OBA researched and considered options for implementing multi-factor authentication for the current MyPBA application. None of the options are feasible given the cost and the planned modernization of the system. Since the alternative analysis will feed into a proposed solution to modernize MyPBA, OBA plans to implement multi-factor authentication with the modernized MyPBA. The modernization effort is slated to start in FY2019. In the interim, as an added precaution for plan participants, we have removed the ability for participants to create an account on-line through MyPBA. Participants must now call our customer contact center to create a MyPBA account.

Thank you for providing us the opportunity to provide this update. If you have questions or comments, please contact me at extension 6816.

cc: David Foley
Jennifer Messina
Bob Scherer
Vidhya Shyamsunder
Marty Boehm

List of PBGC OIG's Risk Advisory and Management Advisory Reports

Report Title	Report Number	Issue Date
Additional Measures to Address Fraud Vulnerabilities in Benefits Administration	SR-2020-07	01/21/2020
OIG Special Report-Additional Safeguards are Needed to Protect Sensitive Participant Data from Insider Threats	SR-2019-09/RA-19-001	03/18/2019
OIG Risk Advisory-Data Protection Considerations for the Field Office Support Services Procurement	SR-2018-15	09/11/2018
OIG Risk Advisory and Management's Response-MyPBA Web Application Control Weaknesses	PA-16-115/RA-2018-03	11/15/2017
OIG Risk Advisory-Personally Identifiable Information and Data Loss Prevention Control Weaknesses		06/28/2017
OIG Risk Advisory and Management's Response - Required Disclosures by Technical Evaluation Panel		12/09/2016
Risk Advisory and Management's Response - Multiemployer Bundled Administrative Expenses in Financial Assistance Requests		07/11/2016
Risk Advisory and Management's Response – Multiemployer Expert Consulting Contracts		02/19/2016
Risk Advisory – ME Program Financial Assistance Review Process		09/30/2015
Management Advisory Report - Ensuring the Integrity of Policy Research and Analysis Department's Actuarial Calculations		05/21/2012