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-trusteed 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.