June 20, 2018

MEMORANDUM TO THE BOARD OF DIRECTORS

FROM: Robert A. Westbrooks
Inspector General

SUBJECT: Special Report No. SR-2018-14
Summary and Analysis of IT Audit Recommendations and the Corporation's Federal Information Security Modernization Act (FISMA) Performance

This special report is to provide the Board with a summary and analysis of the Pension Benefit Guaranty Corporation's progress in remediating IT audit recommendations, as well as its FISMA performance in general and its FISMA performance in comparison to other federal agencies. This report is for informational purposes only.

Summary

The Corporation has made marked improvement in remediating IT weaknesses and deficiencies affecting the independent public accounting (IPA) firm's opinion on internal control in the past five years. In FY 2013, the Corporation had two IT-related material weaknesses in internal control that resulted in 37 audit recommendations. By FY 2017, the Corporation was successful in mitigating these weaknesses to one significant deficiency with seven audit recommendations.

The number of open FISMA-related audit recommendations—which includes both new and prior year unimplemented recommendations—has declined from 64 in FY 2014 to 41 in FY 2017. The number of FISMA-related audit recommendations requiring more than a year to remediate, however, has increased over the last year.

The Corporation's FISMA maturity (OIG assessment) for the past two years ranks as average in comparison to small agencies. In FY 2017, our office rated the Corporation as "not effective" based on the Office of Management and Budget (OMB) scoring criteria. The Corporation was separately rated overall as "managing risk" under the OMB/Department of Homeland Security FISMA risk management assessment, with two of the five domain areas rated as "at risk." This is above average for small agencies.

Overall, we commend management for the progress. More work remains and continued focus and efforts are needed to ensure further improvements in the Corporation's information security posture. The Corporation also needs to swiftly adopt the latest NIST federal security standards and OMB requirements to remain agile in the rapidly changing threat environment.

Background

The Corporation's annual financial statement audit is performed by an IPA firm and our office monitors and reviews the IPA's audit work. As part of the annual financial statement audit, the IPA examines the effectiveness of the internal controls over financial reporting and reports on deficiencies. We also contract with the IPA to perform the annual FISMA evaluation, and we monitor this audit work as well. The IPA leverages some of the work it conducts during the financial statement audit to complete the FISMA evaluation.

IT audit recommendations that are developed during the financial statement audit appear in the annual report on internal control. FISMA-related audit recommendations appear in a separate FISMA evaluation report or the vulnerability assessment and penetration report. While these reports serve different purposes, they should be assessed in the aggregate to ensure a more complete audit perspective on the Corporation's information security posture.

A deficiency in internal control over financial reporting exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis.

A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness, yet important enough to merit attention by those responsible for oversight of the company's financial reporting.

A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis.

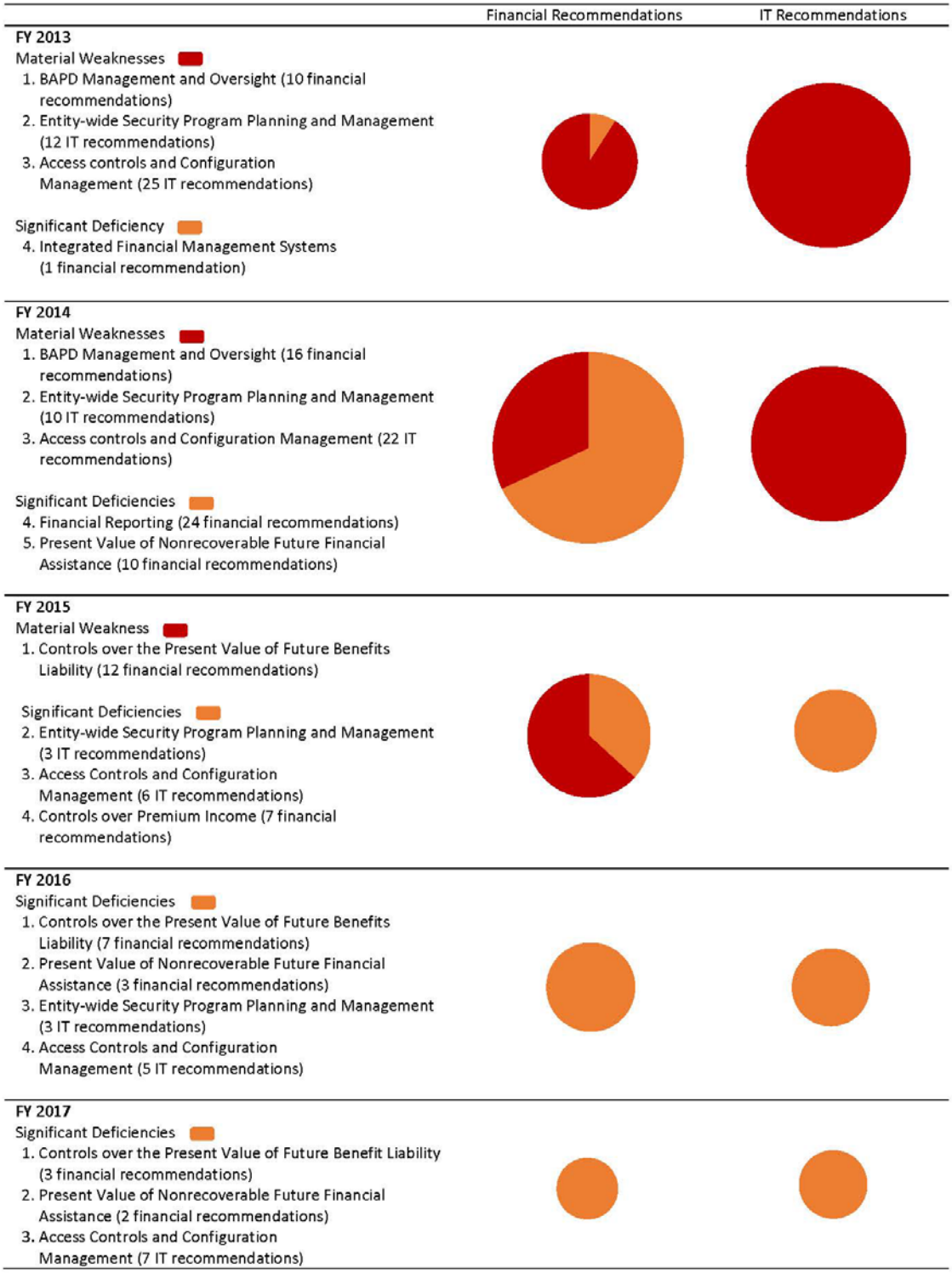
Analysis

IT Audit Recommendations Associated with the Annual Financial Statement Audit

From FY 2013 to FY 2017, the number of open IT-related audit recommendations associated with findings affecting the financial statement audit opinion on internal control has declined.

The impact on the internal control opinion has lessened, and the number of IT and financial audit recommendations has decreased (see fig. 1).

Figure 1: PBGC's Progress in Remediating Weaknesses in Internal Control Over Financial Reporting

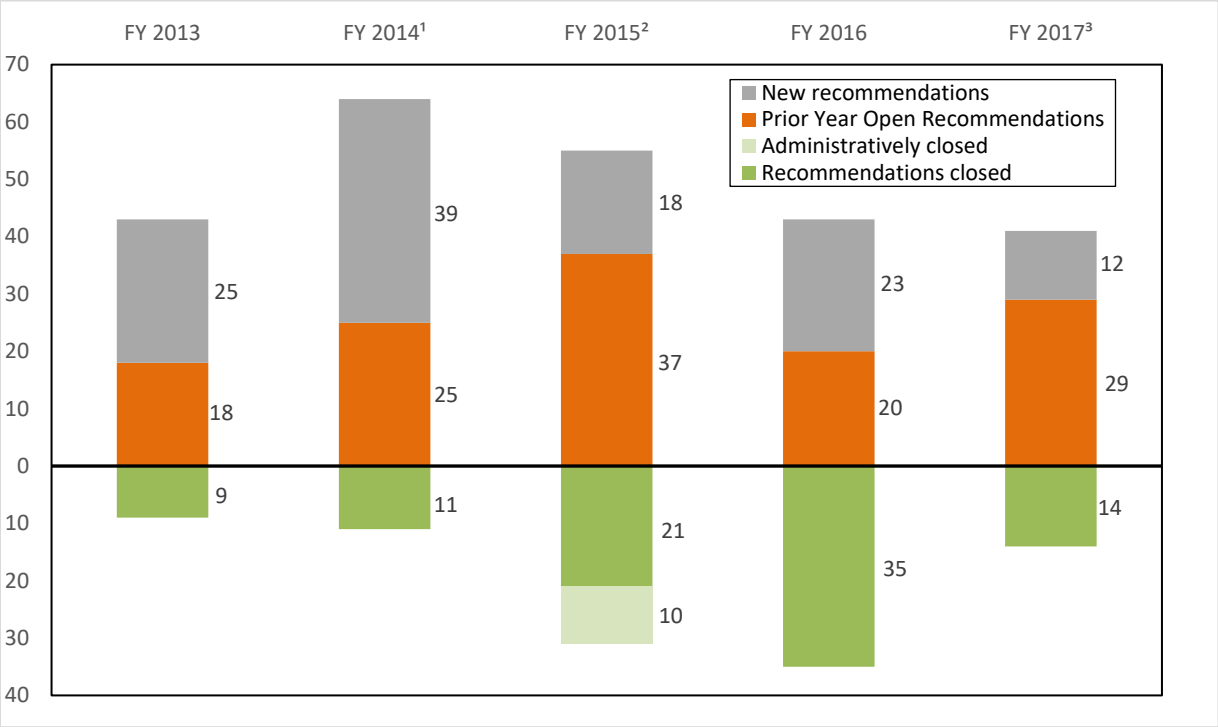


Source: OIG Analysis | SR-2018-14

The Corporation's FISMA Performance

The Corporation was successful in reducing the total number of open FISMA-related audit recommendations from a five-year high of 64 in FY 2014 to five-year low of 41 in FY 2017 (see fig. 2). The Corporation's FY 2017 performance also included a decrease in FISMA-related audit recommendations closed during the year, and an increase in FISMA-related recommendations open for more than a year. PBGC officials explained that OIT has limited resources and must prioritize them. In FY 2017, management focused on improving the IT security posture and closing one of the IT significant deficiencies.

Figure 2: Five-Year Trend of Open and Closed FISMA-Related Audit Recommendations



[1] Seven recommendations were moved to the *Report on Internal Controls Related to the Pension Benefit Guaranty Corporation's Fiscal Year 2014 and 2013 Financial Statements Audit.*
[2] Four recommendations were moved from prior year reports on internal controls to *the Fiscal Year 2015 Federal Information Security Modernization Act Final Report* as prior year recommendations.
[3] One recommendation was moved from a prior year reports on internal controls to *the Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report* as a current year recommendation.

Source: OIG Analysis | SR-2018-14

OMB publishes an Annual Report to Congress in accordance with FISMA. These reports contain individual summaries of agencies' cybersecurity performance. The Corporation's FY 2017 Annual Cybersecurity Risk Management Assessment is attached as Appendix II.

OMB previously provided tables to compare agency performance. These tables were eliminated beginning with the FY 2016 report. We constructed comparison tables from the data contained in the past two FISMA Annual Reports to Congress to aid the Board in its governance role.

OMB, in coordination with DHS, developed a process to evaluate the degree to which agencies manage their cybersecurity risk at the enterprise level. OMB released its methodology for this process as part of OMB Memorandum M-17-25, *Reporting Guidance for Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.

The risk assessments leverage the FY 2017 FISMA CIO metrics and OIG metrics in domains that correspond with each of the five NIST Cybersecurity Framework function areas:

- **Identify** (Asset Management and Authorization; Comprehensive Risk Management)
- **Protect** (Remote Access Protection; Credentialing and Authorization; Network Protection)
- **Detect** (Anti-Phishing Capabilities; Malware Defense Capabilities; Exfiltration and Other Capabilities)
- **Respond** (Planning and Processes; Evaluation and Improvement)
- **Recover** (Planning and Testing; Personal Impact Process; Back-Up Capacity)

In FY 2016, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), in consultation with the Federal Chief Information Officer, jointly worked together to align the OIG FISMA reporting metrics with the NIST Cybersecurity Framework and introduce the maturity model for the areas of information security continuous monitoring and incident response. The purpose of the CIGIE maturity model was to summarize the agencies information security program on a 5-level scale, provide transparency to users of the OIG FISMA reports, and to help ensure consistency across OIGs in their annual FISMA reviews. In FY 2017, OMB extended the maturity model to the remaining function areas and reorganized the models to be more intuitive. For this reason, only the FY 2016 and FY 2017 OIG ratings are included in this report. OMB previously provided tables to compare agency cybersecurity performance in two groups: CFO Act agencies and small agencies. These tables were eliminated beginning with the FY 2016 report. We prepared the *pro forma* comparison tables to aid the Board in determining the Corporation's relative performance to both small agencies and CFO Act agencies.

Figure 3 shows PBGC's *pro forma* ranking among small agencies in FY 2016 and FY 2017 (OIG Rating), and Figure 4 shows PBGC's *pro forma* ranking among CFO Act agencies (OIG Rating).

Figure 5 shows PBGC's *pro forma* ranking among small agencies in FY 2017 (OMB/DHS Risk Management Assessment Rating), and Figure 6 shows PBGC's *pro forma* ranking among CFO Act agencies (OMB/DHS Risk Management Assessment Rating).

PBGC ranks as average among small agencies in the OIG assessment, and above average in the OMB/DHS assessment. While progress has been made, there is room for further improvement.

To be rated "effective" by the OIG under the OMB criteria, an agency's IT security must be rated Managed and Measurable (Level 4). For FY 2017, our office assessed the Corporation at level 3 (Consistently Implemented) for four of the five domains, and at level 2 (Defined) for the other domain. Under the OMB criteria, this results in an overall rating of "not effective."

(remainder of page left blank)

Figure 3: PBGC's *Pro Forma* FISMA Maturity Ranking Among Small Agencies (OIG Rating)

Agency	Identify		Protect		Detect		Respond		Recover	
	2016	2017	2016	2017	2016	2017	2016	2017	2016	2017
Federal Housing Finance Agency										
Federal Energy Regulatory Commission										
Equal Employment Opportunity Commission										
Federal Labor Relations Authority										
Commodity Futures Trading Commission										
National Transportation Safety Board										
Selective Service System										
Tennessee Valley Authority										
International Boundary and Water Commission										
Office of Special Counsel										
Armed Forces Retirement Home										
Farm Credit Administration										
Consumer Financial Protection Bureau										
Defense Nuclear Facilities Safety Board										
Export-Import Bank of the United States										
Federal Maritime Commission										
International Trade Commission										
Millennium Challenge Corporation										
Board of Governors of the Federal Reserve System										
National Credit Union Administration										
Pension Benefit Guaranty Corporation										
Overseas Private Investment Corporation										
Federal Communications Commission										
National Endowment for the Humanities										
Consumer Product Safety Commission										
Corporation for National and Community Service										
Federal Trade Commission										
Inter-American Foundation										
Securities and Exchange Commission										
Chemical Safety Board										
Federal Deposit Insurance Corporation										
Merit Systems Protection Board										
Railroad Retirement Board										
Smithsonian Institution										
Court Services and Offender Supervision Agency										
National Labor Relations Board										
Peace Corps										
Broadcasting Board of Governors										
Denali Commission										
Federal Retirement Thrift Investment Board										
National Archives and Records Administration										
National Endowment for the Arts										

Source: OIG Analysis | SR-2018-14

Figure 4: PBGC's Pro Forma FISMA Maturity Ranking Among CFO Act Agencies (OIG Rating)

Agency	Identify		Protect		Detect		Respond		Recover	
	2016	2017	2016	2017	2016	2017	2016	2017	2016	2017
National Science Foundation										
Nuclear Regulatory Commission										
Department of Homeland Security										
Agency for International Development										
Department of Energy										
General Services Administration										
Department of the Interior										
Department of Justice										
Department of Treasury										
Department of Veterans Affairs										
Environmental Protection Agency										
Department of Labor										
Pension Benefit Guaranty Corporation										
Department of Commerce										
Office of Personnel Management										
Department of Education										
Department of Health and Human Services										
Department of Housing and Urban Development										
Small Business Administration										
Social Security Administration										
Department of Agriculture										
Department of Transportation										
National Aeronautics and Space Administration										
Department of State										

Source: OIG Analysis | SR-2018-14

Legend for Fig. 3 and 4 - OIG FISMA Maturity Rating Scale

	Level 1: Ad-hoc - Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
	Level 2: Defined - Policies, procedures, and strategies are formalized and documented but not consistently implemented.
	Level 3: Consistently Implemented - Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
	Level 4: Managed and Measurable - Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organizations and used to assess them and make necessary changes.
	Level 5: Optimized - Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs.

Figure 5: PBGC's *Pro Forma* FISMA Ranking Among Small Agencies (OMB/DHS Risk Management Assessment)

Agency	Identify	Protect	Detect	Respond	Recover	Overall
Commodity Futures Trading Commission						
Federal Energy Regulatory Commission						
Federal Housing Finance Agency						
International Boundary and Water Commission						
Federal Maritime Commission						
International Trade Commission						
Selective Service System						
Equal Employment Opportunity Commission						
Export-Import Bank of the United States						
Pension Benefit Guaranty Corporation						
Securities and Exchange Commission						
Tennessee Valley Authority						
Armed Forces Retirement Home						
Board of Governors of the Federal Reserve System						
Defense Nuclear Facilities Safety Board						
Farm Credit Administration						
Federal Communications Commission						
Federal Labor Relations Authority						
National Credit Union Administration						
National Labor Relations Board						
National Transportation Safety Board						
Office of Special Counsel						
Overseas Private Investment Corporation						
Federal Deposit Insurance Corporation						
Federal Trade Commission						
Millennium Challenge Corporation						
National Archives and Records Administration						
National Endowment for the Humanities						
Consumer Financial Protection Bureau						
Consumer Product Safety Commission						
Corporation for National and Community Service						
National Endowment for the Arts						
Peace Corps						
Chemical Safety Board						
Federal Retirement Thrift Investment Board						
Inter-American Foundation						
Railroad Retirement Board						
Broadcasting Board of Governors						
Court Services and Offender Supervision Agency						
Denali Commission						
Merit Systems Protection Board						
Smithsonian Institution						

Source: OIG Analysis | SR-2018-14

Figure 6: PBGC's Pro Forma FISMA Ranking Among CFO Act Agencies (OMB/DHS Risk Management Assessment)

Agency	Identify	Protect	Detect	Respond	Recover	Overall
Department of Justice						
General Services Administration						
Nuclear Regulatory Commission						
Agency for International Development						
Department of Education						
Department of Homeland Security						
Department of Labor						
Department of Treasury						
National Science Foundation						
Office of Personnel Management						
Department of Housing and Urban Development						
Department of the Interior						
Pension Benefit Guaranty Corporation						
Social Security Administration						
Department of Energy						
Department of Veterans Affairs						
Department of Commerce						
Department of Health and Human Services						
National Aeronautics and Space Administration						
Small Business Administration						
Department of Agriculture						
Department of State						
Department of Transportation						
Environmental Protection Agency						

Source: OIG Analysis | SR-2018-14

Legend for Fig. 5 and 6 – OMB/DHS Risk Management Assessment Rating Scale

	High Risk: Key, fundamental cybersecurity policies, processes, and tools are either not in place or sufficiently deployed creating a high risk environment for the agency's information systems.
	At Risk: Some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain that place agency information security at risk of compromise.
	Managing Risk: The agency has instituted required information security policies, procedures, and tools and is able to actively manage the cybersecurity risk to the enterprise.

Conclusion

In sum, management has made progress in recent years in addressing cybersecurity risks. This progress has included remediating weaknesses and deficiencies by addressing associated IT audit recommendations affecting the IPA firm's opinion on internal control and reducing the total number of open FISMA-related audit recommendations. Opportunities exist to reduce the number of FISMA-related audit recommendations requiring more than a year to remediate, and to continue to mature the Corporation's cybersecurity program in relation to the FISMA metrics.

Appendix I: Objective, Scope, and Methodology

Objective

Our objective was to provide an information-only report to the Board of Directors with a summary and analysis of the Pension Benefit Guaranty Corporation's progress in remediating FISMA-related audit recommendations and its standing among other federal agencies.

Scope

To answer our objective, we analyzed OIG reports and related data for the five-year period from FY 2013 to FY 2017. We also analyzed OMB's annual FISMA Reports to Congress. We conducted this review from April through June 2018 in Washington, DC.

Methodology

To accomplish our objective, we prepared *pro forma* rankings of agencies FISMA performances for FY 2016 and FY 2017. Consistent with previous OMB reports, we prepared separate tables for small agencies and CFO Act agencies. We also performed an analysis of FISMA-related recommendations during the period.

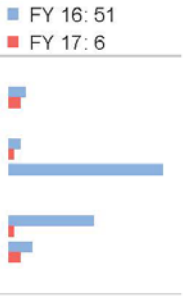
We conducted this project under the authority of the Inspector General Act of 1978, as amended, and in accordance with the Quality Standards for Inspection and Evaluation issued by the Council of the Inspectors General on Integrity and Efficiency.

Appendix II: PBGC's FY 2017 Annual Cybersecurity Risk Management Assessment

FY 2017 Annual Cybersecurity Risk Management Assessment
Pension Benefit Guaranty Corporation

Framework	RMA Rating	IG Rating
Overall	Managing Risk	
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Defined
Detect	At Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover	Managing Risk	Consistently Implemented

Incidents by Attack Vector	FY 16	FY 17
Attrition	0	0
E-mail	3	2
External/Removable Media	0	0
Improper Usage	2	1
Loss or Theft of Equipment	27	0
Physical Cause	NA	0
Web	15	1
Other	4	2
Multiple Attack Vectors	0	0



CIO Risk Management Self-Assessment

Risks | The Pension Benefit Guaranty Corporation (PBGC) has identified its General Support System and two other major applications as HVAs. Potential risk factors to the agency include:

- Delays in modernizing legacy systems to increase cybersecurity resilience;
- Continued use of technology at or near End of Service Life;
- Insufficient resources to acquire adequate cybersecurity workforce;
- Lack of an effective continuous monitoring program;
- Inadequate attention by the Corporation's workforce regarding emerging threats such as phishing, ransomware, and social engineering;
- Less than optimal security hardening of hardware and software;
- Inability to detect and prevent insider threats; and
- Excessive time to deploy security patches.

Strategy | PBGC manages its risks by developing risk mitigation plans, creating Plans of Action and Milestones, implementing mitigation plans, and accepting risks where operational constraints exist.

PBGC also employs programmatic strategies and approaches that ensure PBGC systems are compliant with the Corporation's Information Security Program and applicable laws and regulations. PBGC has established an IT RMF process to align with the NIST RMF. This PBGC RMF emphasizes managing risk at three different tiers: corporation-wide, at the business/mission processes, and within information systems.

Resources | The Corporation is planning to request additional resources for the replacement of IT Infrastructure components that have reached or are reaching end-of-service-life and present critical cybersecurity and functional risks.

PBGC will need supplemental funding for additional support staff to fully implement the NIST Cybersecurity Framework core functions.

Leadership | The ECD provides program status updates to the CIO monthly, and the CIO periodically briefs executives from each business unit about cybersecurity risks impacting their program.

The CIO sponsors the PBGC Cybersecurity and Privacy Council led by the CISO and comprised of Federal Information System Security Managers from the Corporation's business units and the Chief Privacy Officer with the goal of sharing information and making recommendations pertaining to cybersecurity to senior leadership.

Inspector General Assessment

In FY 2017, PBGC's information security program was not effective. PBGC made improvements on its entity-wide security management and access control and configuration management weaknesses but the functional areas were not at a managed and measurable maturity level. PBGC has implemented its Information Security RMF Process and filled its Risk Management Officer position, in addition to requiring strong authentication for all privileged users and almost all non-privileged users. PBGC also redefined its training program to address open recommendations which required additional cycle time to verify the effectiveness of the new monitoring process. The Corporation, however, still needs to ensure accounts are maintained in accordance with PBGC policy, unsupported software is removed, and continued focus is provided to ensure that its flaw remediation process continues to improve on the timely remediation of vulnerabilities and application of necessary patches.