Office of Inspector General
Pension Benefit Guaranty Corporation

October 11, 2019

MEMORANDUM TO THE BOARD OF DIRECTORS

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

SUBJECT: Summary and Analysis of the Corporation's FY 2018 Federal Information Security Modernization Act (FISMA) Performance and Update on IT Remediation Efforts (Special Report No. SR-2020-01)

FISMA requires that the Inspector General perform an annual independent evaluation of the effectiveness of an agency's information security program, practices, and internal controls. We issued our report on the Corporation's FY 2018 performance on December 20, 2018, and that report is available at https://oig.pbgc.gov/pdfs/FA-18-127-4.pdf. Under FISMA, the Office of Management and Budget (OMB) is required to summarize the results of these evaluations across government in an annual report to Congress. The OMB FY 2018 report to Congress was delayed until August 20, 2019. We are issuing this special report to provide the Board with insights from the OMB annual report on the Corporation's cybersecurity performance in relation to the established FISMA metrics and other federal agencies. We note this information represents the Corporation's cybersecurity effectiveness at a point in time; and, therefore, have also included an update on management's IT remediation efforts to date. Our FY 2019 FISMA evaluation report is expected to be issued in January 2020.

This report is for informational purposes only.

Summary

While the Corporation improved its performance in the Protect and Respond functions from the prior year, its overall cybersecurity performance independent assessment rating remains at "not effective" based on the OMB scoring criteria. In FY 2018, 97 agencies were included in the report to Congress but only 84 agencies had IG and independent auditor assessments. By comparison, 42 of the 97 agencies whose data is included in the OMB report were assessed at "effective."

In FY 2018, the Corporation's cybersecurity performance independent assessment ranked above average in comparison to both other small agencies and to CFO Act agencies. This is an improvement in PBGC's performance relative to other agencies.

To address open IT audit recommendations, management has submitted audit recommendation closure packages for 39 of the 48 IT audit recommendations. These packages are pending auditor's review and will be assessed as part of the FY 2019 FISMA evaluation.

While more work remains and continued vigilance is required, we recognize management's attention and efforts to improve the Corporation's information security program, controls, and practices.

Background

In accordance with FISMA, and in coordination with the Department of Homeland Security (DHS), OMB issues annual FISMA reporting guidance. This guidance changes from year to year.

The Corporation's annual financial statement audit is performed by an independent public accounting firm (IPA) 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 control 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.

In FY 2016, OMB, DHS, the Council of the Inspectors General for Integrity and Efficiency (CIGIE), and the Federal Chief Information Officer, collaborated to align the OIG FISMA reporting metrics with the NIST Cybersecurity Framework and introduce a maturity model for two function areas of information security: continuous monitoring and incident response. The purpose of the maturity model was to summarize the agency's information security program on a 5-level scale, provide transparency to users of the IG FISMA reports, and to help ensure consistency across IGs in their annual FISMA evaluations. In FY 2017, the maturity model was extended to the remaining function areas and the models were reorganized to be more intuitive.

In its annual report to Congress, OMB organizes an agency's cybersecurity performance into five components: the Chief Information Officer (CIO) rating, the CIO self-assessment, the independent IG rating, the independent IG assessment, and a count of cybersecurity incidents.

Analysis

PBGC's FY 2018 Cybersecurity Performance Summary

The Corporation's FY 2018 Annual Cybersecurity Performance Summary is attached as Appendix II.

The Corporation's information security program was rated as "at risk" based on the CIO FISMA metrics. This means some essential policies, processes, and tools are in place to mitigate overall cybersecurity risk, but significant gaps remain.

Our office assessed the Corporation at level 3 ("consistently implemented") for four of the five domains, and at a level 4 for the other domain. Under the IG metrics, this results in an overall rating of "not effective." To be rated "effective" under the independent IG assessment, an agency's cybersecurity performance must be rated level 4 ("managed and measurable"). This means that quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess them and make necessary changes. We concluded that the Corporation has implemented many of its policies, procedures, and strategies; but to be effective it still needed to establish and incorporate quantitative and qualitative measures for four of the five functional domains.

The Corporation had one cybersecurity incident in FY 2018, down from 51 cybersecurity incidents in FY 2016.

Table 1 below summarizes the Corporation's improvements from FY 2017.

(remainder of page left blank)

Table 1. PBGC's Improvements in Cybersecurity Performance Independent Assessment from FY 2017

Function	Metric Domains	FY 2017 IG Rating	FY 2018 IG Rating	Trend
Identify	Risk Management	Consistently Implemented (3)	Consistently Implemented (3)	→
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training	Defined (2)	Consistently Implemented (3)	↗
Detect	Information Security Continuous Monitoring	Consistently Implemented (3)	Consistently Implemented (3)	→
Respond	Incident Response	Consistently Implemented (3)	Managed and Measurable (4)	↗
Recover	Contingency Planning	Consistently Implemented (3)	Consistently Implemented (3)	→
Overall		*Not Effective*	*Not Effective*	→

Source: OIG Analysis | SR-2018-14 and OMB FY 2018 Report to Congress

PBGC's FY 2018 FISMA Cybersecurity Performance in Relation to Other Agencies

In prior years, OMB provided tables to compare agency performance in two groups: CFO Act agencies and small agencies. These tables were eliminated beginning with the FY 2016 report. Because comparison data provides perspective and context, we constructed comparison tables from the data contained in the past three OMB annual reports to aid the Board in its governance role.

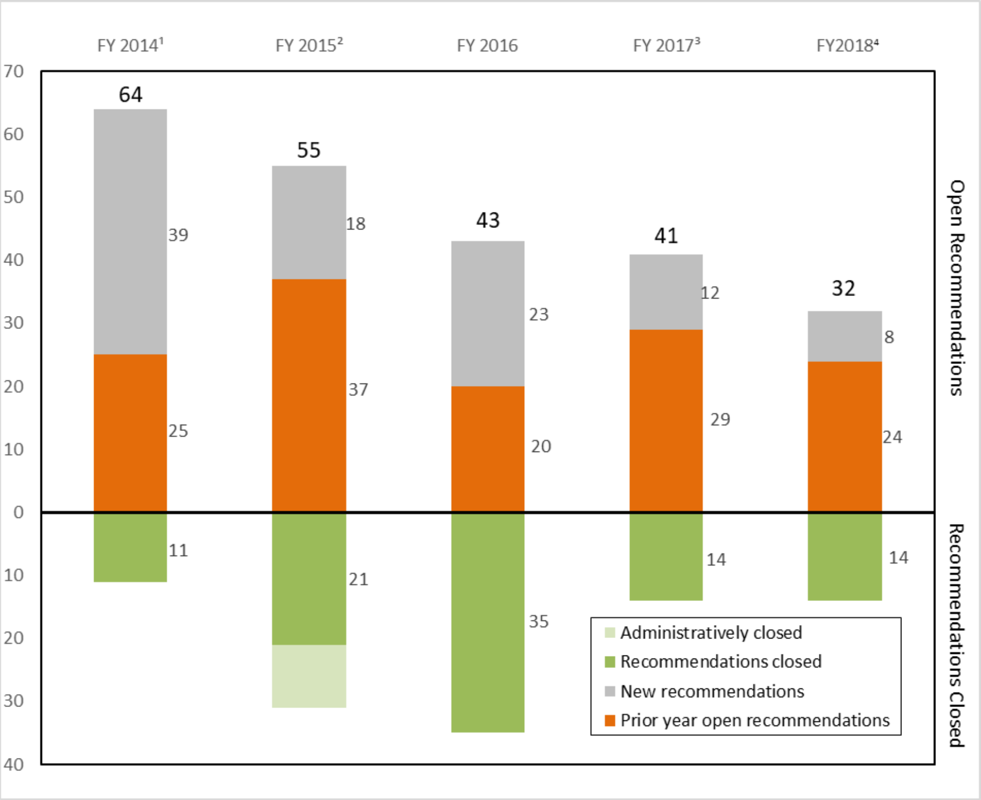
Appendix III shows PBGC's ranking among small agencies in FY 2016 to FY 2018 based on IG independent assessment rating, and Appendix IV shows PBGC's ranking among CFO Act agencies. PBGC ranks above average in these rankings for FY 2018. Among small agencies, the

Corporation's cybersecurity performance independent assessment ranked 19 out of 46. Compared to CFO Act agencies, the Corporation ranked 8 out of 24.

Management's Progress in Addressing Open IT Audit Recommendations

From FY 2014 to FY 2018, the Corporation has reduced the total number of open FISMA and Vulnerability Assessment and Penetration Test (VAPT) audit recommendations from 64 in FY 2014 to 32 in FY 2018 (see figure 1).

Figure 1: Five-Year Trend of Open and Closed FISMA and VAPT Audit Recommendations



Source: OIG Analysis | SR-2020-01

[1] Recommendation actions correspond to actions reported in respective fiscal year reports. Seven recommendations were moved to the Report on Internal Control 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 control 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 control to the Fiscal Year 2017 Federal Information Security Modernization Act Independent Evaluation Report as a current year recommendation.

[4] Three recommendations were moved to the Audit of the Pension Benefit Guaranty Corporation's Fiscal Year 2018 and 2017 Financial Statements report.

Not all IT audit recommendations are from the FISMA and VAPT reports. Through our FY 2018 Financial Statement Audit, FISMA and VAPT reports, we have issued a total of 13 new IT audit recommendations. We closed 19 IT audit recommendations. There were 48 total open IT audit recommendations at the beginning of the FY 2019 Financial Statement and FISMA audits.

Of the 48 open IT audit recommendations, management has submitted closure packages for 39, of which one has been closed and 38 are pending auditor's review as of September 30, 2019. This review involves rigorous scrutiny and evaluation of the audit artifacts submitted by management to ensure management has taken sufficient corrective action to address the recommendation and that there has been sufficient cycle time to demonstrate the operating effectiveness of the corrective action. We caution that we typically return as insufficient between 20-30 percent of submitted closure packages.

Management has submitted closure packages for the two oldest open IT audit recommendations, both dating back to 2007. One of these recommendations was issued to remedy vulnerabilities noted in key databases and applications such as weaknesses in configuration, roles, privileges, auditing, file permissions, and operating system access (OIG Control No. FS-07-14). This recommendation was originally issued to address issues noted within Oracle systems. While management had taken some corrective actions over the years, similar issues were identified in other systems which prevented the auditors from agreeing to close the recommendation. The other oldest open IT audit recommendation called for management to implement a logging and monitoring process for application security related events and critical system modifications (OIG Control No. FS-07-17). While management had taken some corrective actions over the years, recurring issues were identified which prevented the auditors from agreeing to close this recommendation. In November 2018, we revised the wording of this recommendation to provide greater clarity on what management action will be required to close the recommendation. We commend management for submitting closure packages for these two long-standing open recommendations, while reserving judgment on the sufficiency of the corrective action pending auditor's review.

The three oldest open IT audit recommendations for which there are no closure packages under auditor's review are from 2015. One of these recommendations is from the restricted disclosure vulnerability assessment and penetration test report (OIG Control OIT-154R). According to management, based on availability of funding labor resources were not obtained to operate this program until late FY 2018. The program is underway but will require additional cycle time to support a closure package. Management estimates that it will submit a closure package by June 2020. The second recommendation required management to develop, document and implement a process to timely determine whether the risk-level for employees or contractors changed when transferring them to a new role. PBGC reported that the process mapping was being completed and required adequate time for testing. Management expects to submit a completion package early in FY 2020. The other open 2015 IT audit recommendation called for management to complete the implementation of enterprise security common controls. Common controls are security controls whose implementation results in a security capability that is inheritable by one or more PBGC information systems. Management reports that is has completed implementation of 286 of 299 (96 percent) common controls as of September 2019 and estimates that it will submit a closure package by June 2020.

Conclusion

The Corporation has improved its cybersecurity performance over the past several years and is above average among federal agencies according the annual FISMA data. More work remains and continued vigilance is required. The Corporation needs to continue to swiftly implement new federal cybersecurity requirements, diligently address open IT audit recommendations, and aggressively respond to emerging threats.

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

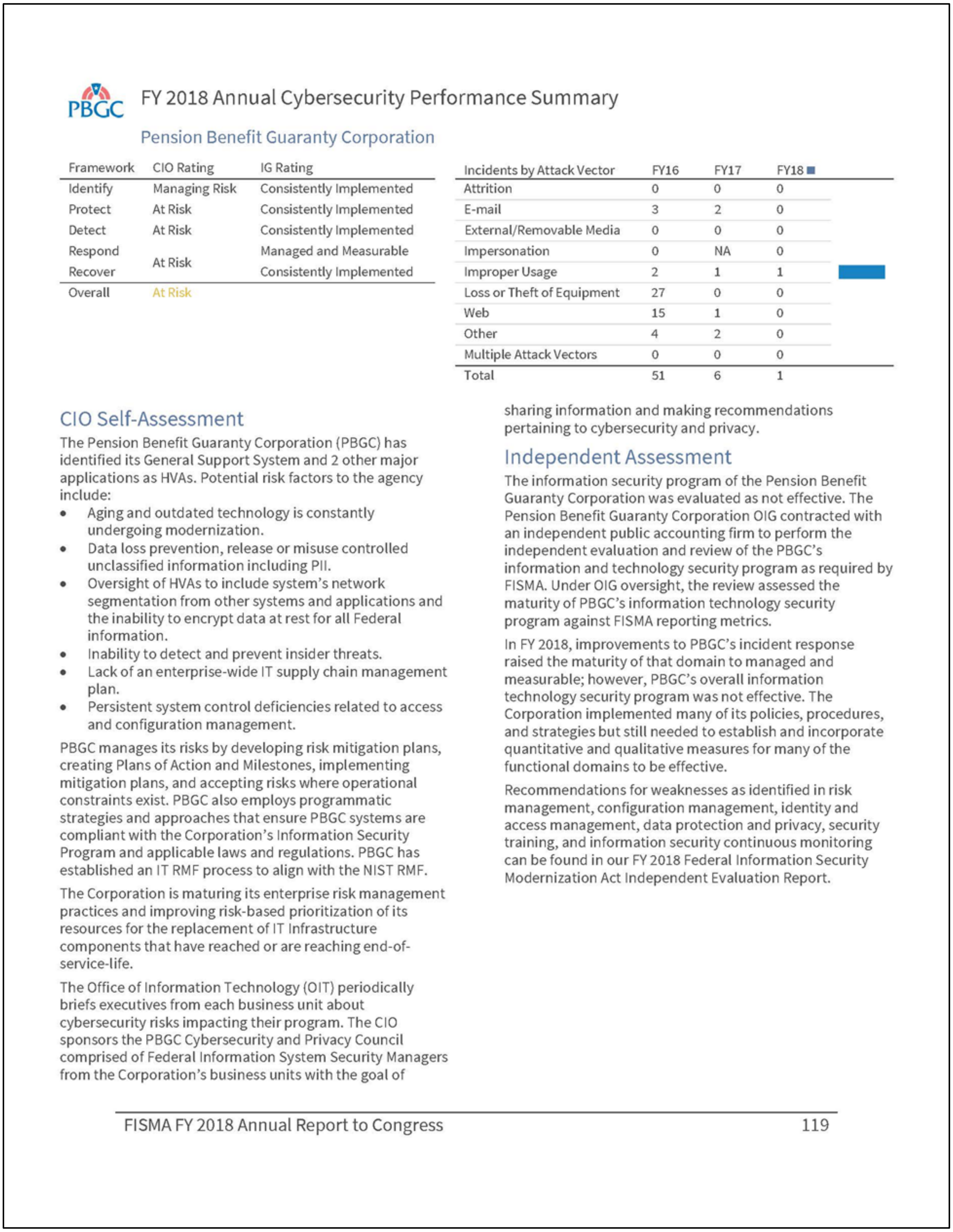
To answer our objective, we analyzed OIG reports and related data for the five-year period from FY 2014 to FY 2018. We also analyzed OMB's annual FISMA Reports to Congress. We conducted this review from August through September 2019 in Washington, DC.

Methodology

To accomplish our objective, we prepared *pro forma* rankings of agencies FISMA performances for FY 2016 to FY 2018. Consistent with previous OMB reports, we prepared separate tables for small agencies and CFO Act agencies.

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 2018 Annual Cybersecurity Performance Summary



FY 2018 Annual Cybersecurity Performance Summary

Pension Benefit Guaranty Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Consistently Implemented
Detect	At Risk	Consistently Implemented
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	At Risk	

Incidents by Attack Vector	FY16	FY17	FY18 ■
Attrition	0	0	0
E-mail	3	2	0
External/Removable Media	0	0	0
Impersonation	0	NA	0
Improper Usage	2	1	1
Loss or Theft of Equipment	27	0	0
Web	15	1	0
Other	4	2	0
Multiple Attack Vectors	0	0	0
Total	51	6	1

CIO Self-Assessment

The Pension Benefit Guaranty Corporation (PBGC) has identified its General Support System and 2 other major applications as HVAs. Potential risk factors to the agency include:

- Aging and outdated technology is constantly undergoing modernization.
- Data loss prevention, release or misuse controlled unclassified information including PII.
- Oversight of HVAs to include system's network segmentation from other systems and applications and the inability to encrypt data at rest for all Federal information.
- Inability to detect and prevent insider threats.
- Lack of an enterprise-wide IT supply chain management plan.
- Persistent system control deficiencies related to access and configuration management.

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.

The Corporation is maturing its enterprise risk management practices and improving risk-based prioritization of its resources for the replacement of IT Infrastructure components that have reached or are reaching end-of-service-life.

The Office of Information Technology (OIT) periodically briefs executives from each business unit about cybersecurity risks impacting their program. The CIO sponsors the PBGC Cybersecurity and Privacy Council comprised of Federal Information System Security Managers from the Corporation's business units with the goal of sharing information and making recommendations pertaining to cybersecurity and privacy.

Independent Assessment

The information security program of the Pension Benefit Guaranty Corporation was evaluated as not effective. The Pension Benefit Guaranty Corporation OIG contracted with an independent public accounting firm to perform the independent evaluation and review of the PBGC's information and technology security program as required by FISMA. Under OIG oversight, the review assessed the maturity of PBGC's information technology security program against FISMA reporting metrics.

In FY 2018, improvements to PBGC's incident response raised the maturity of that domain to managed and measurable; however, PBGC's overall information technology security program was not effective. The Corporation implemented many of its policies, procedures, and strategies but still needed to establish and incorporate quantitative and qualitative measures for many of the functional domains to be effective.

Recommendations for weaknesses as identified in risk management, configuration management, identity and access management, data protection and privacy, security training, and information security continuous monitoring can be found in our FY 2018 Federal Information Security Modernization Act Independent Evaluation Report.

Appendix III: PBGC's FY 2016 to FY 2018 Cybersecurity Maturity Ranking Among Small Agencies (IG Assessment)

	2016					2017					2018				
Agency	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**	**Identify**	**Protect**	**Detect**	**Respond**	**Recover**
Federal Energy Regulatory Commission	5	5	3	2	5	5	4	5	4	3	5	5	5	4	3
Federal Housing Finance Agency	5	5	4	4	5	5	4	5	5	5	4	4	5	4	3
Commodity Futures Trading Commission	3	3	5	4	5	3	4	5	3	4	3	4	4	4	4
Office of Special Counsel	2	2	1	2	5	4	4	4	3	3	4	4	4	4	3
Selective Service System	5	5	5	5	3	4	4	4	4	3	4	4	4	4	3
Equal Employment Opportunity Commission	3	3	2	3	5	5	4	4	3	4	4	3	4	4	3
Farm Credit Administration	4	4	2	2	5	4	4	3	3	3	4	4	3	3	4
National Transportation Safety Board	5	3	5	5	3	4	3	4	4	4	4	3	4	4	3
Overseas Private Investment Corporation	3	2	3	2	5	2	3	2	3	3	4	3	4	4	3
Tennessee Valley Authority	2	3	1	2	3	4	4	3	4	4	4	4	2	4	4
Consumer Financial Protection Bureau	4	3	3	3	3	3	3	4	3	3	3	3	4	4	3
Federal Labor Relations Authority	3	3	4	5	5	4	4	4	4	4	3	4	4	3	3
Institute of Museum and Library Services	3	3	2	4	5	4	4	4	4	4	3	3	4	4	3
International Boundary and Water Commission	5	5	2	2	5	4	4	3	3	4	2	4	3	4	4
International Trade Commission	2	3	2	1	2	3	3	3	3	3	4	3	4	3	3
Board of Governors of the Federal Reserve	2	3	2	1	3	2	3	3	3	3	2	4	3	4	3
Federal Maritime Commission	5	3	4	5	5	3	3	3	3	3	3	3	4	3	3
Millennium Challenge Corporation	4	3	2	3	5	3	3	3	3	3	4	3	3	3	3
Pension Benefit Guaranty Corporation	3	3	2	3	3	3	2	3	3	3	3	3	3	4	3
Armed Forces Retirement Home	5	3	1	2	3	3	4	3	4	3	3	4	2	4	2
Defense Nuclear Facilities Safety Board	3	3	1	1	1	3	3	3	3	3	3	3	3	3	3
Election Assitance Commission	5	3	2	1	5	3	2	2	2	2	4	3	2	3	3
Inter-American Foundation	2	3	1	1	1	3	2	2	1	3	3	3	3	3	3
American Battle Monuments Commission	2	2	3	2	2	2	3	2	2	2	3	3	3	3	2
Federal Trade Commission	3	3	2	3	2	2	3	2	2	2	3	3	2	3	3
National Credit Union Administration	2	2	2	1	3	2	2	3	3	4	2	3	3	3	3
Corporation for National and Community Service	3	2	2	2	1	2	2	2	3	2	2	3	2	3	3
Export-Import Bank of the United States	2	1	2	2	5	4	3	2	3	3	3	3	3	2	2
Federal Communications Commission	1	2	2	3	2	3	2	2	2	3	3	4	2	2	2
National Endowment for the Humanities	3	3	2	3	2	2	3	2	3	2	2	4	2	3	2
African Development Foundation	1	1	2	2	2	1	2	2	3	3	2	2	2	3	3
Federal Deposit Insurance Corporation	3	3	2	1	3	2	2	2	2	2	1	3	2	3	3
National Labor Relations Board	3	2	1	1	3	1	1	2	1	1	1	2	2	3	3
Smithsonian Institution	1	1	1	1	1	1	2	2	2	1	2	3	2	2	2
Chemical Safety Board	5	3	3	2	5	2	2	2	2	2	2	2	2	2	2
Consumer Product Safety Commission	1	1	2	1	1	1	1	4	4	1	1	2	2	4	1
Securities and Exchange Commission	2	2	2	3	3	2	2	2	2	3	2	2	2	2	2
National Archives and Records Administration	1	1	1	1	2	1	1	1	1	1	2	1	2	2	2
Court Services and Offender Supervision Agency	1	1	2	1	1	1	2	1	1	2	1	2	1	2	2
Merit Systems Protection Board	2	1	1	1	5	2	2	2	2	2	3	1	2	1	1
Federal Retirement Thrift Investment Board	1	1	1	1	2	1	1	1	1	1	1	2	1	1	1
Peace Corps	1	1	1	2	1	1	1	1	2	1	1	1	1	2	1
Denali Commission	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
National Endowment for the Arts	3	3	3	4	1	1	1	1	1	1	1	1	1	1	1
Railroad Retirement Board	3	1	1	2	2	2	1	1	3	1	1	1	1	1	1
U.S. Agency for Global Media	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Appendix IV: PBGC's FY 2016 to FY 2018 Cybersecurity Maturity Ranking Among CFO Act Agencies (IG Assessment)

	2016					2017					2018				
Agency	Identify	Protect	Detect	Respond	Recover	Identify	Protect	Detect	Respond	Recover	Identify	Protect	Detect	Respond	Recover
National Science Foundation	3	3	4	4	5	4	4	4	4	4	4	4	4	4	4
Agency for International Development	2	3	2	3	5	4	4	2	3	3	5	4	3	4	3
Department of Homeland Security	3	3	3	3	3	4	3	3	4	3	4	4	4	4	3
Nuclear Regulatory Commission	2	2	2	1	3	4	4	4	4	3	4	4	4	4	3
General Services Administration	3	3	3	4	3	3	3	3	4	3	4	3	3	4	3
Department of Energy	2	2	1	1	1	3	3	3	4	3	3	3	3	4	3
Department of Justice	3	3	3	3	4	3	3	3	3	3	3	3	3	4	3
Pension Benefit Guaranty Corporation	3	3	2	3	3	3	2	3	3	3	3	3	3	4	3
Department of Labor	2	2	2	1	5	3	3	3	2	3	3	3	3	3	3
Department of the Interior	2	2	1	1	2	3	4	3	2	3	3	4	3	2	3
Department of Treasury	2	2	1	1	3	3	3	3	3	3	3	3	3	3	3
Department of Veterans Affairs	2	3	2	3	3	3	3	2	4	3	3	3	2	4	3
Environmental Protection Agency	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3
Department of Commerce	2	3	1	2	3	3	2	2	4	2	2	2	4	4	2
Department of Education	5	2	1	1	5	3	2	2	2	2	3	2	2	2	3
Department of Health and Human Services	3	2	3	3	3	2	2	2	3	2	3	3	2	2	2
Office of Personnel Management	2	2	3	3	2	2	3	2	4	2	1	3	2	4	2
Social Security Administration	2	2	3	3	3	2	2	2	2	3	2	3	2	2	3
Department of Housing and Urban Development	2	3	2	2	2	2	3	2	2	2	2	2	2	3	2
Department of Agriculture	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2
Department of Transportation	2	2	1	1	2	2	2	2	2	2	2	2	2	2	2
National Aeronautics and Space Administration	2	1	1	2	2	2	2	2	2	2	2	2	2	2	2
Department of State	1	1	1	1	1	1	2	1	2	1	1	2	1	3	2
Small Business Administration	2	2	2	2	5	3	2	2	2	2	2	2	2	2	1

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.