Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

MEMORANDUM

DATE: April 29, 2020

TO: Donna Roy
Chief Information Officer
Bureau of Consumer Financial Protection

FROM: Peter Sheridan
Associate Inspector General for Information Technology

SUBJECT: OIG Report 2020-IT-C-014: Testing Results for the Bureau's Plan of Action and Milestones Process

Executive Summary

We are issuing this memorandum to bring to your attention opportunities to strengthen the Bureau of Consumer Financial Protection's plan of action and milestones (POA&M) process for managing cybersecurity weaknesses. Specifically, we found that costs associated with remediating cybersecurity weaknesses listed in POA&Ms were not accurately accounted for. We also identified instances in which the status of cybersecurity weaknesses included in the Bureau's automated solution for POA&M management was inaccurate. These issues may hamper the Bureau's ability to effectively allocate resources to ensure the timely remediation of cybersecurity weaknesses and impair its performance reporting related to POA&M items.

We identified these issues as part of our 2019 audit of the Bureau's information security program, conducted pursuant to the requirements of the Federal Information Security Modernization Act of 2014 (FISMA).[1] We did not report this information in our 2019 FISMA audit report because it did not affect the Bureau's information security program maturity rating.[2] However, we believe that this information can

[1] Office of Inspector General, *2019 Audit of the Bureau's Information Security Program*, OIG Report 2019-IT-C-015, October 31, 2019.

[2] In accordance with the U.S. Department of Homeland Security's *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, we are required to determine the maturity of the Bureau's information security program, including its POA&M process; however, the areas identified in this memorandum report are not specifically a component of the maturity determination. U.S. Department of Homeland Security, *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*, Version 1.3, April 9, 2019.

assist with the Bureau's ongoing efforts to strengthen its risk management program and the maturity of its POA&M process.

Our memorandum contains two recommendations designed to strengthen the Bureau's process for managing cybersecurity weaknesses. In its response to our draft memorandum, the Bureau concurs with our recommendations and outlines actions that have been or will be taken to address them. We will follow up to ensure that the recommendations are fully addressed.

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Recommendations, 2020-IT-C-014, April 29, 2020

Testing Results for the Bureau's Plan of Action and Milestones Process

Finding 1: Costs of Remediating POA&M Items Are Inconsistently Tracked

Number	Recommendation	Responsible office
1	Ensure that system owners are accurately estimating and accounting for costs associated with remediating security weaknesses listed in POA&Ms.	Office of Technology and Innovation

Finding 2: The Status of POA&M Items Is Not Accurately Reflected in the Bureau's Automated Solution

Number	Recommendation	Responsible office
2	Work with system owners to ensure that evidence to close system-level cybersecurity weaknesses listed in POA&Ms are submitted in a timely manner and that the weaknesses' status is accurately reflected in the Bureau's automated solution.	Office of Technology and Innovation

Background

FISMA requires federal agencies to develop and implement a POA&M process to document and remediate information security weaknesses. National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (SP 800-53), further states that agencies must develop POA&Ms for their information systems to document planned and remedial actions so that security weaknesses or deficiencies can be corrected and known vulnerabilities in the system reduced or eliminated. The publication notes that organizations should employ automated mechanisms to help ensure that the POA&Ms for their information systems are accurate, up to date, and readily available.[3]

To meet FISMA and NIST requirements, the Bureau has developed a *Plan of Action and Milestones (POA&M) Management Process* document for the remediation of information security program- and system-level weaknesses. The document outlines a POA&M process consisting of three phases: development, maintenance, and reporting (table 1). These phases cover recording of all program- and system-level weaknesses in a POA&M, identifying funding requirements necessary to mitigate weaknesses, and status reporting of POA&M-related activities.[4] The Bureau also uses an automated solution to facilitate POA&M phases and activities.

Table 1. The Bureau's POA&M Process

POA&M Phase	Activities
Development	• Identify weaknesses • Determine root cause • Categorize weaknesses • Handle risk-based exceptions • Document the corrective action plans • Determine resource and funding requirements and availability • Prioritize remediation • Assign completion dates
Maintenance	• Update the POA&M • Validate completion of remediation efforts • Retire and transfer POA&M line items
Reporting	• Produce weekly, monthly, quarterly, and annual reports

Source: OIG analysis of the Bureau's *POA&M Management Process*.

[3] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, Special Publication 800-53, Rev. 4, April 2013.

[4] The Bureau's *POA&M Management Process* notes that a program-level weakness is one that that has been identified as being systemic to the information security program because it affects the enterprise, has broad reuse as a common or hybrid control, or is common to multiple systems. It also notes that a system-level weakness arises from a specific management, operational, or technical control deficiency in a particular system. Each system weakness is entered individually on a system-specific POA&M.

Scope and Methodology

The objective of our 2019 FISMA audit was to evaluate the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. To support our objectives, we analyzed Bureau policies and procedures, including the *CFPB Information Security Program Policy* and *POA&M Management Process*. We also reviewed the Bureau's information security program-level POA&M and POA&Ms for the agency's information systems, including those that are cloud based. We judgmentally sampled 25 of 83 open POA&M items rated *Very High* or *High* in the Bureau's automated solution to determine whether the Bureau's POA&M process was operating effectively.[5] We also met with Bureau staff responsible for managing and remediating POA&Ms.

Finding 1: Costs of Remediating POA&M Items Are Inconsistently Tracked

We found that the costs of remediating POA&M items are not accurately accounted for. Specifically, of a sample of 25 POA&M items rated *Very High* or *High*, 16 items had an identified cost that did not accurately reflect the level of effort needed. For example, weaknesses related to cryptographic protections and encryption had inaccurately low remediation costs listed in the Bureau's automated solution. Bureau officials stated that costs for POA&M items are entered because *cost* is a required field in the Bureau's automated solution, but some items may not have an actual cost associated with them. Bureau officials also stated that they are working on a plan to improve the tracking of costs for POA&M items.

The Bureau's *POA&M Management Process* states that the system owner must determine the cost of POA&M remediation activities. Cost estimates should include the costs of hardware, software, labor, and other related costs. We believe that by accurately accounting for the costs associated with POA&M items, the Bureau will be better able to allocate resources to ensure the timely mitigation of the most-critical security weaknesses. Further, in our previous audits, Bureau officials have cited a lack of resources as a contributing factor for issues we identified—for example, a finding in our 2018 FISMA report related to the timely remediation of technical vulnerabilities.[6] Additionally, in our report, *The Bureau Can Improve the Effectiveness of Its Lifecycle Processes for FedRAMP*, we found that the Bureau did not ensure that continuous monitoring activities were effectively performed for selected cloud systems.[7] Bureau officials informed us that the lack of continuous monitoring activities resulted from a lack of formal policies, procedures, and resources. As such, we believe that the accurate identification of costs to mitigate

[5] According the Bureau's *POA&M Management Process*, POA&M items are assigned one of four risk levels: *Critical*, *High*, *Medium*, or *Low*. The Bureau uses *Critical* and *Very High* synonymously for tracking their highest-risk severity items. The document further states that system owners and information system security managers should consider available information, such as risk analysis and assessment, scanning results, and other credible information, to determine the risk level of POA&M items.

[6] Office of Inspector General, *2018 Audit of the Bureau's Information Security Program*, OIG Report 2018-IT-C-018, October 31, 2018.

[7] Office of Inspector General, *The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP*, OIG Report 2019-IT-C-009, July 17, 2019.

security weaknesses could also provide the Bureau with important information to inform resource allocation decisions.

Recommendation

We recommend that the chief information officer (CIO)

1. Ensure that system owners are accurately estimating and accounting for costs associated with remediating security weaknesses listed in POA&Ms.

Management Response

The CIO concurs with this recommendation. The CIO notes that the Cybersecurity Team has developed overall cost estimates for resources needed to remediate each NIST control. The CIO states that the next steps are to begin assisting system owners in estimating their costs to remediate weaknesses listed in their POA&Ms, and then update the estimated cost of closing each POA&M.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Finding 2: The Status of POA&M Items Is Not Accurately Reflected in the Bureau's Automated Solution

We found that system owners were not ensuring that the status of POA&M items was accurately reflected in the Bureau's automated solution.[8] Specifically, we sampled 25 system-level POA&M items classified as *Very High* or *High* and found that the status of 11 items was inaccurate.[9] The cybersecurity weaknesses for these 11 POA&M items had been remediated; however, system owners did not submit the required documentation for closure. As such, these 11 weaknesses were showing as open in the Bureau's automated solution when they should have been closed. Such instances negatively affect the Bureau's performance reporting on the status of POA&M activities across the agency and may hinder the agency's ability to allocate resources to remediate unaddressed weaknesses in a timely manner.

The Bureau's *POA&M Management Process* notes that the system owner is responsible for overseeing the successful remediation of each weakness documented in the POA&M. Further, the system owner, in conjunction with the designated information system security manager (ISSM), is responsible for gathering and documenting evidence in support of weakness remediation efforts. Lastly, after remediating a POA&M item, the system owner submits corresponding evidence to the designated ISSM for concurrence. The ISSM then updates the status of the POA&M items in the Bureau's automated solution. Bureau officials who oversee the POA&M process noted that they had sent reminders to system owners

[8] The Bureau's *POA&M Management Process* notes that the status of POA&M items can be one of five options: *not started*, *in progress*, *complete*, *closed*, or *deviation*.

[9] We provided the details of the specific 11 POA&M items to Bureau officials in a separate, restricted communication.

on POA&M remediation efforts but had not received timely responses. Specifically, system owners were not submitting evidence to close POA&M items in a timely manner. We believe that the timely submission of evidence to close POA&Ms, once remediation activities are completed, would allow for more-accurate performance reporting and enable the Bureau to more effectively allocate resources to mitigate POA&M items.

Recommendation

We recommend that the CIO

2. Work with system owners to ensure that evidence to close system-level cybersecurity weaknesses listed in POA&Ms are submitted in a timely manner and that the weaknesses' status is accurately reflected in the Bureau's automated solution.

Management Response

The CIO concurs with this recommendation. The CIO notes that the Cybersecurity Team has developed a POA&M maturation plan, approved by the chief operating officer, to enhance the POA&M management process. The CIO states that the plan includes, but is not limited to, expectations of the system owners, remediation enforcement activities, and management escalation points. Further, the CIO notes that the Bureau has established weekly system owner meetings to discuss all open weaknesses, weekly POA&M metric reports that are provided to the chief information security officer and the CIO, and a monthly briefing to the director.

OIG Comment

We believe that the actions described by the Bureau are responsive to our recommendation. We plan to follow up on the Bureau's actions to ensure that the recommendation is fully addressed.

Conclusion

In accordance with FISMA, the Bureau has developed and implemented a POA&M process to manage program- and system-level cybersecurity weaknesses. We identified opportunities to further improve the agency's POA&M process by ensuring that costs to mitigate security weaknesses are accurately accounted for and that the status of POA&M items is accurately reflected in the Bureau's automated solution. In its response to our draft report, the Bureau concurs with our recommendations and outlines actions that have been or will be taken to address them. We have included the Bureau's response as an attachment to this memorandum. We will continue to monitor the agency's progress in strengthening its POA&M process as part of our future FISMA reviews.

We appreciate the cooperation that we received from your staff during our review. Please contact me if you would like to discuss this report or any related issues.

Attachment
cc: Kirsten Sutton
Kate Fulton

Elizabeth Reilly
Katherine Sickbert
Tiina Rodrigue
Dana James
Lauren Hassouni
Anya Veledar
Carlos Villa

Attachment

Management Response

Bureau of Consumer Financial Protection
1700 G Street NW
Washington, D.C. 20552

April 14, 2020

Mr. Peter Sheridan
Associate Inspector General for Information Technology
Board of Governors of the Federal Reserve System &
Bureau of Consumer Financial Protection
20th and C Streets, NW
Washington, DC 20551

Dear Mr. Sheridan,

Thank you for the opportunity to review and comment on the Office of Inspector General's (OIG) three draft supplemental memos that came from the *2019 Audit of the BCFP's Information Security Program* Report: OIG Technical Testing Results for the Bureau's Remote Access Solution, OIG Testing Results of Select Bureau Cybersecurity Incident Response Processes, and OIG Testing Results for the Bureau's Plan of Action and Milestones Process.

We value your objective, independent viewpoints and consider OIG to be a trusted source of informed, accurate, and insightful information.

Thank you for the professionalism and courtesy that you and all of the OIG personnel demonstrated throughout this review. We have provided comments for each recommendation.

Sincerely,

Digitally signed by Donna Roy
Date: 2020.04.14 13:11:19 -04'00'

Donna Roy
Chief Information Officer

consumerfinance.gov

Response to recommendations presented in the Draft OIG Supplemental Memorandum, "*OIG Testing Results for the Bureau's Plan of Action and Milestones Process.*"

Recommendation 1: Ensure that system owners are accurately estimating and accounting for costs associated with remediating security weaknesses listed in POA&Ms.

Management Response: The Bureau concurs with this recommendation. The Cybersecurity Team has developed overall cost estimates per NIST control for Cybersecurity resources, the next step is to assist System Owners in estimating their costs to remediate weaknesses listed in their POA&Ms. When System Owners finalize their costs CFPB will update the estimated cost associated with closing each of POA&Ms.

Recommendation 2: Work with system owners to ensure that artifacts and evidence to close system-level cybersecurity weaknesses listed in POA&Ms are submitted in a timely manner and that the weaknesses' status is accurately reflected in the Bureau's automated solution.

Management Response: The Bureau concurs with this recommendation. The Cybersecurity team developed a POA&M Maturation plan that was approved by the Chief Operating Officer. The POA&M Maturation Plan enhances the Bureau's POA&M management process that includes, but is not limited to, expectations of the System Owners, remediation enforcement activities, and management escalation points. CFPB has established weekly System Owner meetings to discuss all open weaknesses, weekly POA&M metric reports to provide to the CISO and CIO, and monthly briefing to the Director.