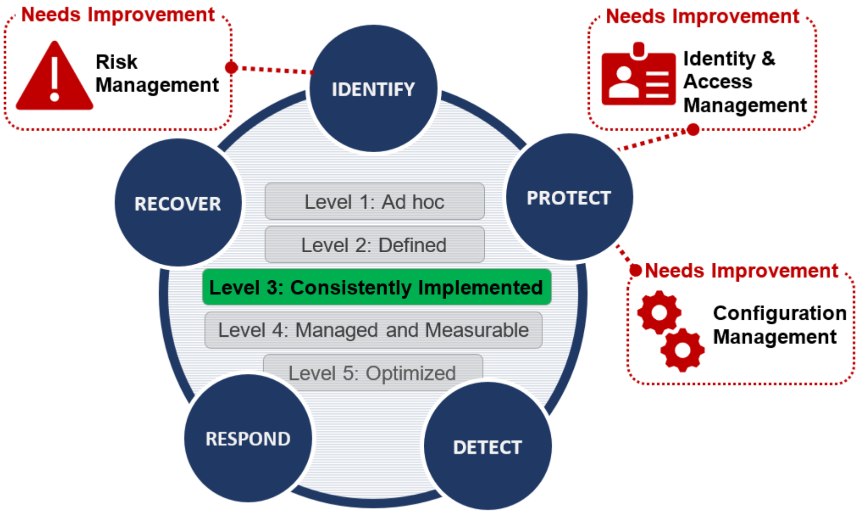
U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL

Compliance with the law
Operating efficiently and effectively

EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users

Report No. 21-E-0124 April 16, 2021



Report Contributors:

Rudolph M. Brevard
LaVonda Harris-Claggett
Eric Jackson Jr.
Alonzo Munyeneh
Jeremy Sigel
Sabrena Stewart

Abbreviations

CIO	Chief Information Officer
EPA	U.S. Environmental Protection Agency
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
ICAM	Identity, Credential, and Access Management
IG	Inspector General
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OMS	Office of Mission Support
U.S.C.	United States Code

Cover Image: The EPA has consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. (EPA OIG image)

Are you aware of fraud, waste, or abuse in an EPA program?

EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW (2431T)
Washington, D.C. 20460
(888) 546-8740
(202) 566-2599 (fax)
OIG_Hotline@epa.gov

Learn more about our OIG Hotline.

EPA Office of Inspector General
1200 Pennsylvania Avenue, NW (2410T)
Washington, D.C. 20460
(202) 566-2391
www.epa.gov/oig

Subscribe to our Email Updates
Follow us on Twitter @EPAoig
Send us your Project Suggestions

U.S. Environmental Protection Agency
Office of Inspector General

21-E-0124
April 16, 2021

At a Glance

Why We Did This Evaluation

We performed this evaluation to assess the U.S. Environmental Protection Agency's compliance with the *FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics*.

The fiscal year 2020 *IG FISMA Reporting Metrics* outlines five security function areas and eight corresponding domains to help federal agencies manage cybersecurity risks. The document also outlines five maturity levels by which IGs should rate agency information security programs:

- Level 1, Ad Hoc.
- Level 2, Defined.
- Level 3, Consistently Implemented.
- Level 4, Managed and Measurable.
- Level 5, Optimized.

This evaluation addresses the following:

- *Compliance with the law.*
- *Operating efficiently and effectively.*

This evaluation addresses top EPA management challenges:

- *Enhancing information technology security.*
- *Complying with key internal control requirements (data quality).*

Address inquiries to our public affairs office at (202) 566-2391 or OIG_WEBCOMMENTS@epa.gov.

List of OIG reports.

EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users

What We Found

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and eight domains outlined in the *FY 2020 IG FISMA Reporting Metrics*. This means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We found that the EPA has deficiencies in the following areas:

Deficiencies in the EPA's information technology internal controls could be used to exploit weaknesses in Agency applications and hinder the EPA's ability to prevent, detect, and respond to emerging cyberthreats.

- Completing reviews of its outdated information security procedures by the established deadlines or making plans to complete a review at a later date.
- Verifying corrective actions are completed as represented by the Agency and not falsely reporting related resolutions.
- Enforcing established information system control requirements for the Agency's web application directory system that allows external users access to EPA applications, including the grants and Superfund management systems.

Recommendations and Planned Agency Corrective Actions

We recommend that the assistant administrator for Mission Support (1) establish a control to update information technology procedures to make them consistent with current federal directives, (2) take steps to require that the audit follow-up coordinator has the capability to verify when corrective actions are completed before the action official closes audit reports in the Agency's audit tracking system, (3) implement a control for authorization and recertifying users' access for the web application directory system, (4) implement procedures to monitor privileged users' activities for unusual or suspicious activity, and (5) establish a governance structure to support the Agency's identity, credential, and access management program efforts as required by the Office of Management and Budget.

The EPA agreed with our five recommendations; completed corrective actions for two of them; and provided acceptable planned corrective actions and estimated milestone dates for the remaining three, which we consider resolved with corrective actions pending.

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

April 16, 2021

MEMORANDUM

SUBJECT: EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users
Report No. 21-E-0124

FROM: Sean W. O'Donnell Sean W O'Donnell

TO: Donna J. Vizian, Acting Assistant Administrator
Office of Mission Support

This is our report on the subject evaluation conducted by the Office of Inspector General of the U.S. Environmental Protection Agency. The project number for this evaluation was OA&E-FY20-0033. This report contains findings that describe the problems the OIG has identified and corrective actions the OIG recommends. Final determinations on matters in this report will be made by EPA managers in accordance with established audit resolution procedures.

The Office of Mission Support is responsible for the issues discussed in this report.

We issued five recommendations in this report. The Office of Mission Support completed corrective actions for two recommendations and provided acceptable planned corrective actions for three recommendations. In accordance with EPA Manual 2750, all recommendations are completed or resolved with corrective actions pending. No further response is required. However, if you submit a response, it will be posted on the OIG's website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for redaction or removal along with corresponding justification.

We will post this report to our website at www.epa.gov/oig.

Table of Contents

Appendices

Purpose

The Office of Inspector General performed this evaluation to assess the U.S. Environmental Protection Agency's compliance with the fiscal year 2020 inspector general reporting instructions for the Federal Information Security Modernization Act of 2014.

Top Management Challenge

This evaluation addresses the following top management challenges for the Agency, as identified in OIG Report No. 20-N-0231, *EPA's FYs 2020–2021 Top Management Challenges*, issued July 21, 2020:

- Enhancing information technology security.
- Complying with key internal control requirements (data quality).

Background

Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems collected, maintained, or used by or on behalf of the agency.[1]

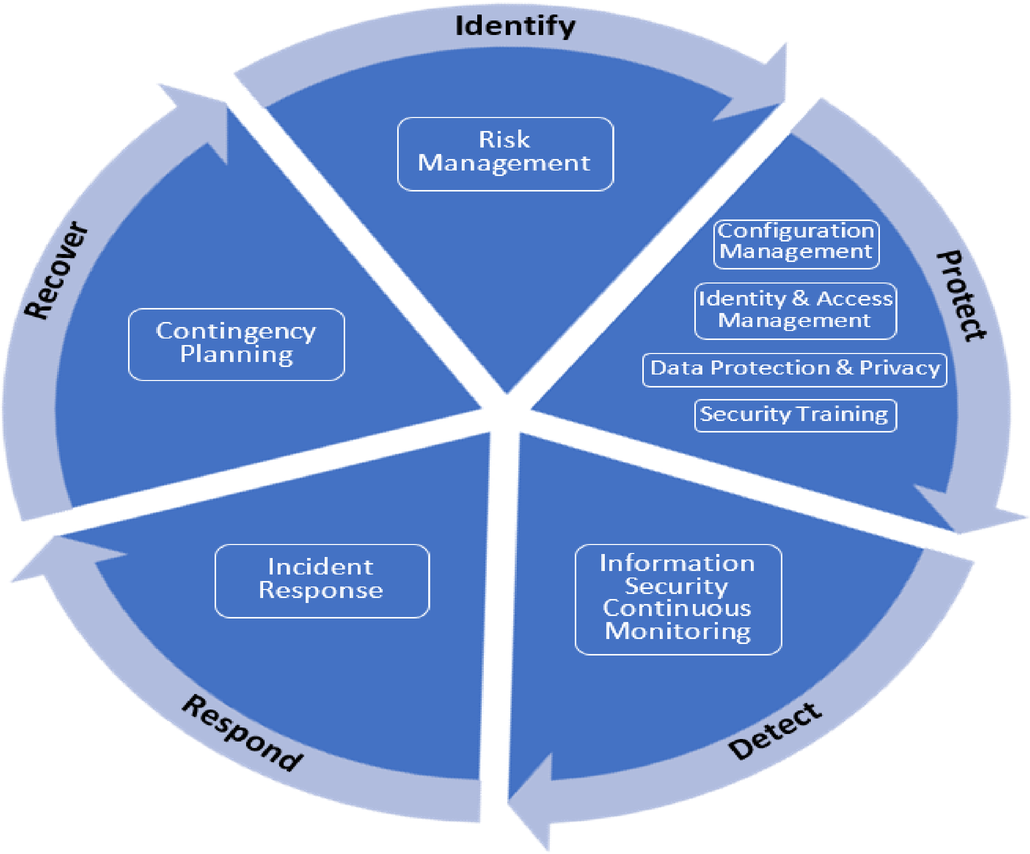
Each fiscal year, the U.S. Department of Homeland Security and the Office of Management and Budget issue the *Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* template to the IG of each federal agency to assess the agency's information security program. These metrics were developed as a collaborative effort among the OMB, the Department of Homeland Security, and the Council of the Inspectors General on Integrity and Efficiency, in consultation with the Federal Chief Information Officer Council. The *FY 2020 IG FISMA Reporting Metrics* identified eight domains within five security function areas defined in the National Institute of Standards and Technology *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, dated April 16, 2018 (Figure 1).[2] The document contains 67 metrics for IGs to assess. These metrics and their assessed ratings can be found in Appendix A.

This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

[1] 44 U.S.C. § 3554(a)(1)(A).

[2] Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, was issued on February 12, 2013, and directed NIST to develop a cybersecurity framework based on existing industry standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

Figure 1: FY 2020 cybersecurity framework—five security functions with eight security domains

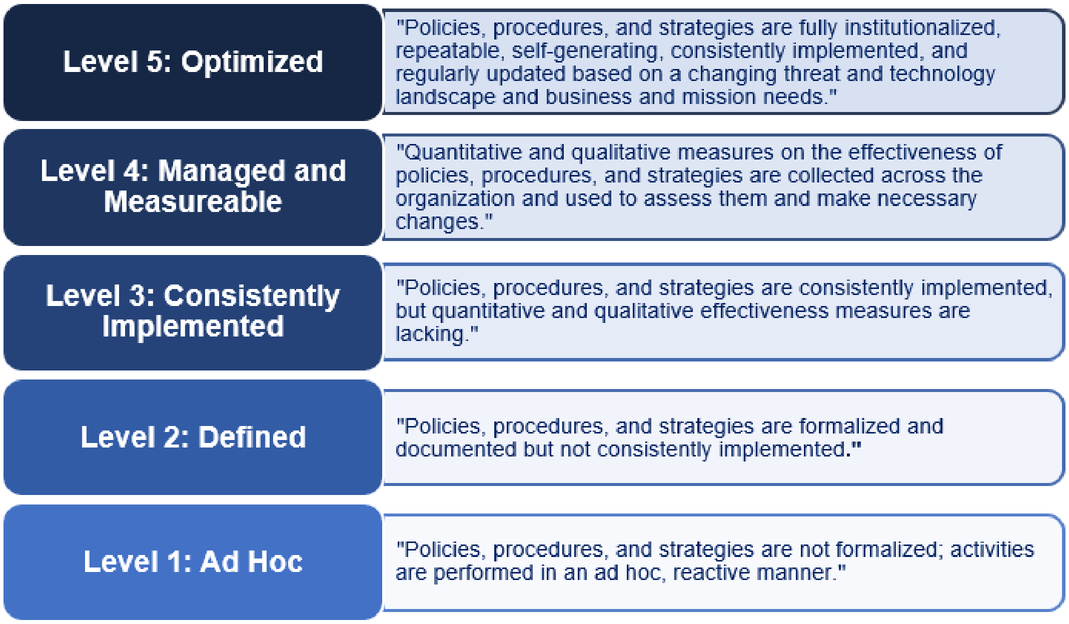


Source: OIG summary of the *FY 2020 IG FISMA Reporting Metrics*. (EPA OIG image)

The effectiveness of an agency’s information security program is based on a five-tiered maturity model spectrum (Figure 2). The IGs are responsible for annually assessing the agency’s rating along this spectrum by determining whether the agency possesses the required policies, procedures, and strategies for each of the eight domains. The IGs make this determination by answering a series of questions about the domain-specific criteria that are presented in the annual *IG FISMA Reporting Metrics* template.

Within the maturity model spectrum, the agency should perform risk assessments and identify the optimal maturity level that achieves cost-effective security when considering the agency’s missions and risks. This approach requires the agency to develop the necessary policies, procedures, and strategies in order to meet effective levels of security, including the more advanced maturity levels (3, 4, and 5) for which the agency has consistently and effectively implemented and institutionalized those policies and procedures.

Figure 2: Maturity model spectrum



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 and mission needs."
Level 4: Managed and Measureable	"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."
Level 3: Consistently Implemented	"Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking."
Level 2: Defined	"Policies, procedures, and strategies are formalized and documented but not consistently implemented."
Level 1: Ad Hoc	"Policies, procedures, and strategies are not formalized; activities are performed in an ad hoc, reactive manner."

Source: *FY 2020 IG FISMA Reporting Metrics*. (EPA OIG image)

Responsible Office

The Office of Mission Support leads the EPA's information management and information technology programs. It is responsible for providing the necessary information, technology, and services to support the Agency's mission. Within the OMS:

- The chief information security officer is responsible for the EPA's information security program and ensures that the program complies with FISMA and other information security laws, regulations, directives, policies, and guidelines.

- The Office of Information Technology Operations owns the Enterprise Identity and Access Management Program, which provides the documentation, confirmation, and approval of individuals using IT resources across the Agency.

Scope and Methodology

We conducted this evaluation from May 2020 to February 2021 in accordance with the *Quality Standards for Inspection and Evaluation* published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency. Those standards require that we perform the evaluation to obtain sufficient, competent, and relevant evidence to provide a reasonable basis for our findings, conclusions, and recommendations based on our objectives. We believe that the evidence obtained provides a reasonable basis for our findings, conclusions, and recommendations.

We assessed whether the EPA implemented the policies and procedures outlined within the *FY 2020 IG FISMA Reporting Metrics* for the FISMA domains within each FISMA security function area. We reviewed the information security reports that the OIG issued in FY 2020 (Appendix B) and reports issued by the U.S. Government Accountability Office to identify weaknesses within the EPA's information security program related to the FY 2020 FISMA metrics. We reviewed EPA policies and procedures to identify significant changes made to the Agency's governance practices that would impact the FY 2020 FISMA metrics. We used this information and compared the FY 2019 and FY 2020 FISMA reporting metrics within our risk assessment to determine our level of testing for this evaluation. We defined a metric as high risk if it met one of the following criteria:

- Our FY 2019 assessment rating of the metric would materially change because of a key change between the FY 2019 and FY 2020 IG FISMA reporting metrics' underlying criteria.

- The metric was rated below Level 3 in the OIG's FY 2019 FISMA audit.

- Our FY 2019 assessment for the metric would materially change because of significant changes to the EPA's information security policies or procedures.

- The metric was under the Identity and Access Management domain relevant to the EPA's COVID-19 readiness, meaning it related to the Agency's ability to respond to IT threats and vulnerabilities and maintain IT operations during the coronavirus pandemic.

Key Definitions

Five **function areas** make up the cybersecurity framework that provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.

Function areas are further broken down into eight **domains** developed to promote consistent and comparable metrics and criteria in the assessment of the effectiveness of the agencies' information security programs.

FISMA reporting guidance consists of 67 **metrics**, which are questions divided among the eight domains to provide reporting requirements across key areas to be addressed in the independent evaluations of agencies' information security programs.

The 67 metrics were developed from **underlying criteria** consisting of OMB, Department of Homeland Security, Council of the Inspectors General on Integrity and Efficiency, and Federal CIO Council guidance and security control requirements relevant to that metric's cybersecurity risk.

NIST's *Framework for Improving Critical Infrastructure Cybersecurity* provides that the Identity and Access Management domain metrics would be met if "Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistently with the assessed risk of unauthorized access to authorized activities and transactions."

For these high-risk metrics, we inquired with Agency personnel, inspected relevant Agency IT documentation, and analyzed evidence supporting EPA compliance with the metrics outlined in the *FY 2020 IG FISMA Reporting Metrics*. We rated the metrics as low risk if they did not meet any of the above criteria. Additionally, if no changes were made to the EPA's policies and procedures and no other issues were identified for a specific metric, we were able to determine the maturity level for the metric based on our FY 2019 FISMA assessment results.

Based on the *FY 2020 IG FISMA Reporting Metrics* reporting instructions, the overall maturity level for each domain is calculated based on a simple majority. For example, if a domain has seven metrics questions and three metrics questions were rated at Level 2 and four metrics questions were rated at Level 3, the domain would be rated at Level 3. This calculation is performed automatically by the OMB's Cyberscope system that the IGs use to report their assessment results. Although IGs have flexibility in determining the overall rating, the *FY 2020 IG FISMA Reporting Metrics* recommends that the agency's overall maturity level be based on a simple majority—the most frequent maturity level assigned to the individual domains serves as the agency's overall maturity rating.

For the Identity and Access Management domain, the EPA identified the Enterprise Identity and Access Management general support system, which consists of multiple subsystems, as the most significant system for identity and access management operations during the coronavirus pandemic. To test this domain, we sampled the general support system's web application directory subsystem because it provides authentication and password policy management capabilities for external users to access the Agency's grants and Superfund management systems. We assessed the web application directory system against the Level 4 (Managed and Measurable) maturity model criteria to determine if the EPA reached this level.

We provided our assessment of each function area of the *FY 2020 IG FISMA Reporting Metrics* and discussed the results with the Agency. Appendix A provides the OIG's assessment for each FISMA metric, as submitted to the OMB on October 29, 2020.

Relevant Audit

We followed up on the three recommendations made in OIG Report No. 20-P-0120, *EPA Needs to Improve Its Risk Management and Incident Response Information Security Functions,* dated March 24, 2020. These recommendations addressed weaknesses found in the OIG's FY 2019 FISMA audit including creating an up-to-date software inventory, establishing controls to validate the timely creation of plans of actions and milestones for vulnerability testing weaknesses, and implementing incident response technologies. We reported that the EPA provided acceptable corrective actions to address our three recommendations, and all recommendations were considered resolved with planned corrective actions pending.

On June 24, 2020, the OMS issued a memorandum to the EPA follow-up official, who is responsible for all of the Agency's audit resolutions, stating that the OMS completed corrective actions for all three recommendations on February 5, 2020. This was false. Our follow-up activities, in fact, determined that the OMS did **not** complete the corrective actions as stated in its memorandum. We discuss our findings in this regard within this report.

Results

We concluded that the EPA achieved an overall maturity level of Level 3 (Consistently Implemented) for the five security functions and eight domains outlined in the *FY 2020 IG FISMA Reporting Metrics* (Appendix C). This means that the EPA consistently implemented its information security policies and procedures, but quantitative and qualitative effectiveness measures are lacking. We found the EPA has deficiencies in its processes for:

- Reviewing Agency IT procedures by their established review dates to ensure procedures were compliant with current federal directives.

- Verifying that personnel completed agreed-to corrective actions before notifying the Agency follow-up official to close the audit report in the Agency's audit tracking system.

- Enforcing established information system security controls requiring web application directory system personnel to:

    - Maintain external users' authorization forms for the web application directory system separately from the approvals for the specific applications the users are accessing.

    - Regularly monitor privileged user activity.

- Establishing a governance structure to support the Agency's identity, credential, and access management program.

OMB Circular A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, states that management is "responsible for establishing and integrating internal controls into its operations … in order to provide reasonable assurance that the entity's internal control over operations, reporting, and compliance is operating effectively." Without internal controls to keep IT procedures current with the latest federal guidance and complete agreed-to corrective actions, the EPA cannot provide reasonable assurance that its information security program is structured to prevent, detect, and respond to emerging cyberthreats. Additionally, the identity and access management control deficiencies found within the reviewed web application directory system could be used to further exploit weaknesses in supported EPA applications to expose Agency data to unauthorized change, loss, or destruction.

Appendix A contains the details of our assessment for each of the five functions and eight domains we reviewed.

EPA Has Not Updated IT Procedures

The EPA has not updated key IT procedures to align with the latest federal directives associated with the protect security function outlined in the NIST *Framework for Improving Critical Infrastructure Cybersecurity*. Specifically, the following EPA procedures were not updated to reflect implementation of the security control requirements as provided in NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*:

- *Interim Configuration Management Procedures*, CIO 2150.3-P-05.1.
- *Interim Personnel Security Procedures*, CIO 2150.3-P-13.1.
- *Interim System and Communications Protection Procedures,* CIO 2150.3-P-16.1.

Table 1: Outdated Agency IT procedure documents

Procedure	Cybersecurity framework security function	CIO approval date	Planned review date
CIO 2150.3-P-05.1 *Information Security – Interim Configuration Management Procedures*	Protect	8/6/12	8/6/15
CIO-2150.3-P-13.1 *Information Security – Interim Personnel Security Procedures*	Protect	8/6/12	8/6/15
CIO 2150.3-P-16.1 *Information Security – Interim System and Communications Protection Procedures*	Protect	8/6/12	8/6/15

Source: OIG analysis. (EPA OIG table)

As illustrated in Table 1, documents for each of the interim procedures were last approved by the CIO on August 6, 2012, and have a review date of August 6, 2015. The procedure documents were not updated because the responsible offices did not review the documents by the established review date to determine whether the EPA should update them.

The EPA created a plan of action and milestones to track the update to the *Interim Configuration Management Procedures* and provided that the update would occur by July 31, 2017. However, the update did not occur by the estimated completion date and completing the plan of action and milestones is over three-and-a-half years overdue. EPA staff stated that updated procedures to comply with Revision 4 were developed but have not completed internal review. Upon our inquiry, EPA staff stated that the *Interim System and Communications Protection Procedures* would be updated by October 30, 2020, and the remaining two procedures would be updated by November 30, 2020. At the time of this evaluation, on February 23, 2021, the EPA's policy and procedures webpage for information security did not include these updated procedures.

Without enforcing established internal controls to review and update IT security control procedures documentation, the Agency cannot ensure that the information security program adheres to current federal requirements for implementing the information system security controls needed to protect the confidentiality, integrity, and availability of EPA systems and data.

Action Officials Inaccurately Report Corrective Actions Completed Without Actions Actually Being Taken

The OMS issued a certification memorandum on June 24, 2020, to the EPA's agency follow-up official inaccurately stating that the office completed all corrective actions for OIG Report No. 20-P-0120. The memorandum stated that corrective actions to address the three recommendations were implemented, and that the implementation was verified by EPA officials. We found that, in fact, corrective actions to address two of the report's three recommendations related to deficiencies in the Agency's risk management program would actually **not** be completed until December 2021.

The EPA's *Manual 2750 Audit Management Procedures* delegates the responsibility and authority for implementing the audit resolution program to the action official. The action official works with the audit follow-up coordinator to ensure corrective actions are documented, implemented, tracked, and reported.

The corrective actions for Recommendation 1 of the report required two separate tasks to address the recommendation; however, the OMS communicated that all tasks were completed after only verifying completion of the first task. This was false. Additionally, the estimated completion date for the corrective actions for Recommendation 2 was revised following communication with the EPA's former chief information security officer and the OIG. The audit follow-up coordinators in OMS reported the recommendation as completed prior to the revised completion date without proper verification.

The EPA is required to complete agreed-to corrective actions to address audit recommendations and accurately document the Agency's activities in compliance with federal and Agency directives. Without completing agreed-to corrective actions to address known security weaknesses, the confidentiality, integrity, and availability of the Agency's systems and data remain at risk. Additionally, erroneously representing remediation of reported deficiencies erodes public confidence in the accuracy and reliability of the Agency's assertions in response to OIG reports.

EPA Lacks a Governance Structure to Support the Identity, Credentials, and Access Management Program that Oversees Operations of the Agency's Web Application Directory System

We assessed the Agency's web application directory system responsible for managing external user access to Agency applications, including the grants and Superfund management systems, for compliance with the Identity and Access Management FISMA domain and found that the EPA did not:

- Follow established authorization processes for a sample of external web application directory system users.[3] The EPA allowed external users access to the web application directory system without documented approval or verification that the users needed access to the system to do their jobs.

- Establish a governance structure to support consistent implementation of the Agency's ICAM processes as required by OMB Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*. It states, "Each agency shall designate an integrated agency-wide ICAM office, team, or other governance structure in support of its Enterprise Risk Management capability to effectively govern and enforce ICAM efforts." Although the Agency's August 2018 ICAM roadmap documented its plan to create an ICAM Project Management Office to fulfill the OMB requirement, the office was not established.

- Monitor privileged user access for unusual or unauthorized activity.

NIST defines a **privileged user** as a user that is authorized to perform security-relevant functions that ordinary users are not authorized to perform.

The findings listed above occurred because:

- The Agency did not have a process to move external users' authorizations to the new version of the web application directory system after the system was updated. Additionally, the EPA did not have a process to recertify that these users still needed access to the system as required by NIST.

[3] See EPA *Information Security – Access Control Procedure*, CIO 2150-P-01.2.

- OMS staff stated that they do not regularly monitor privileged user activity on the web application directory system, even though this requirement is outlined in EPA *Information Security – Audit and Accountability Procedures*, CIO 2150-P-3.3.

- Responsibility for the creation of the Agency's planned ICAM Project Management Office had not been established.

Without enforcing authorizations for EPA systems, the EPA risks the security of its data by granting users access to systems they may not need, compromising the confidentiality of important EPA information and subjecting the data to unauthorized disclosure.

Likewise, privileged users can bypass information system security controls. Without monitoring these users for unusual or suspicious activities, a data breach could occur and privileged users could cover their tracks, making it harder for the EPA to properly respond to the attack or know that a system breach had occurred. Furthermore, without establishing a governance structure, as required by the OMB, the EPA lacks a cohesive method of implementing federal and Agency requirements to implement, manage, and maintain the necessary ICAM policies, processes, and technologies.

Conclusions

While the EPA demonstrated that it had implemented an information security program consistent with the majority of FISMA metrics, the Agency should continue its efforts to maintain a resilient security posture in compliance with the latest federal and Agency policies, procedures, and directives. Improvements in the EPA's IT procedures documentation, audit follow-up processes, and ICAM program are essential to ensure that the EPA can prevent, detect, and respond to emerging cyberthreats and increase the maturity level for these critical elements of information security. In addition, the Agency must accurately report whether it has completed corrective actions resulting from prior reports.

Recommendations

We recommend that the assistant administrator for Mission Support:

1. Update information security procedures to make them consistent with current federal directives, including the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.

2. Establish a process in which the audit follow-up official verifies that corrective actions were completed before the action official certifies that the audit report should be closed in the EPA audit tracking system.

3. Implement procedures for approving and maintaining external users' authorizations to access the web application directory system.

4. Implement procedures to monitor web application directory system privileged users' activities for unusual or suspicious activity.

5. Designate an integrated agencywide identity, credential, and access management office, team, or other governance structure as required by Office of Management and Budget Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*.

Agency Response and OIG Assessment

The EPA agreed with our five recommendations; completed corrective actions for two of them; and provided acceptable planned corrective actions and estimated milestone dates for the remaining three, which we consider resolved with corrective action pending.

For Recommendation 1, the OMS stated that it would update internal policies and procedures to comply with NIST 800-53, Revision 5. The recommendation is resolved with planned corrective action pending.

For Recommendation 3, the OMS stated that it would integrate with Login.gov to provide external user identity vetting and authentication services for the Agency. Additionally, the EPA stated that an external user recertification process will take place during the migration to Login.gov requiring re-registration for the existing user community. Furthermore, the EPA stated that it would develop a periodic external user recertification process to ensure access is limited to current need. Recommendation 3 is resolved with planned corrective action pending.

For Recommendation 4, the OMS stated that it would coordinate with EPA system owners and information security officers to implement processes to monitor privileged users' activities for unusual or suspicious activity. Recommendation 4 is resolved with planned corrective action pending.

The OMS provided acceptable corrective actions for Recommendations 2 and 5, which it completed on March 16, 2021, and November 2, 2020 respectively. We consider these recommendations complete.

The Agency's response to the draft report is in Appendix D.

Status of Recommendations and Potential Monetary Benefits

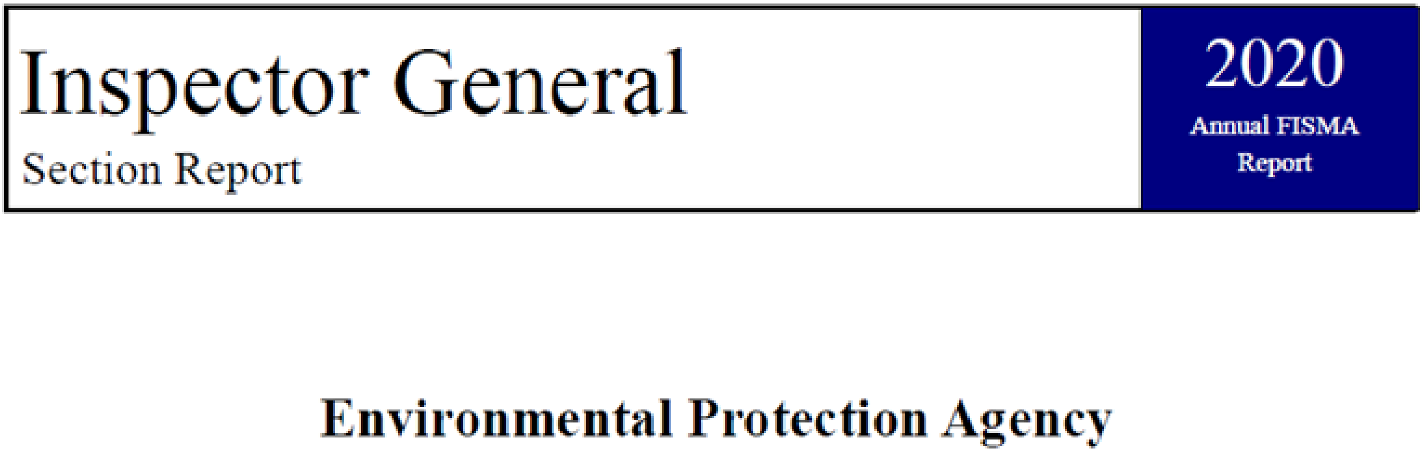
RECOMMENDATIONS

Rec. No.	Page No.	Subject	Status[1]	Action Official	Planned Completion Date	Potential Monetary Benefits (in $000s)
1	10	Update information security procedures to make them consistent with current federal directives, including the National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.	R	Assistant Administrator for Mission Support	6/30/22	
2	10	Establish a process in which the audit follow-up official verifies that corrective actions were completed before the action official certifies that the audit report should be closed in the EPA audit tracking system.	C	Assistant Administrator for Mission Support	3/16/21	
3	11	Implement procedures for approving and maintaining external users' authorizations to access the web application directory system.	R	Assistant Administrator for Mission Support	12/31/21	
4	11	Implement procedures to monitor web application directory system privileged users' activities for unusual or suspicious activity.	R	Assistant Administrator for Mission Support	10/15/21	
5	11	Designate an integrated agencywide identity, credential, and access management office, team, or other governance structure as required by Office of Management and Budget Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*.	C	Assistant Administrator for Mission Support	11/2/20	

[1] C = Corrective action completed.
R = Recommendation resolved with corrective action pending.
U = Recommendation unresolved with resolution efforts in progress.

Appendix A

OIG-Completed CyberScope Template



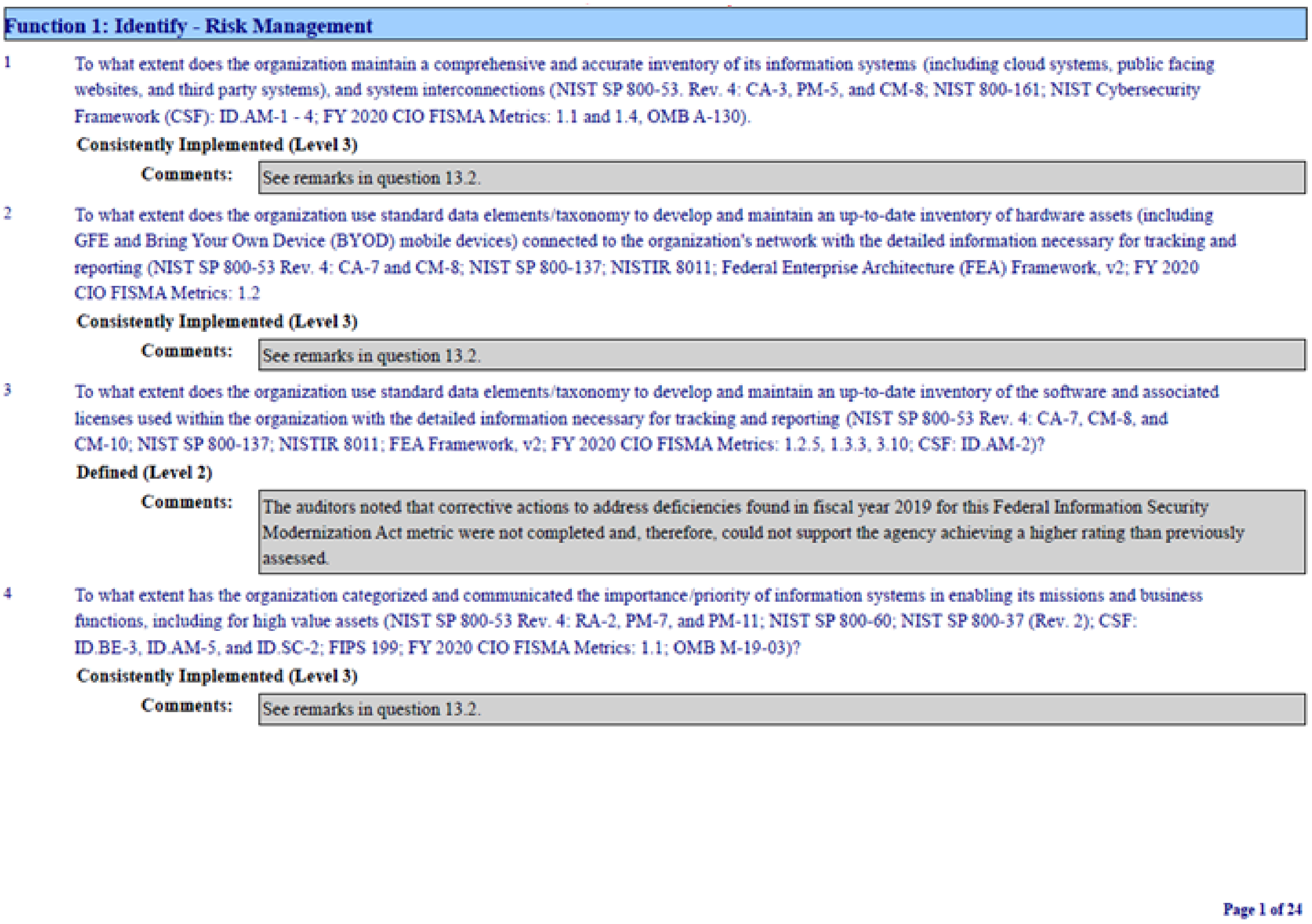
Inspector General

Section Report

2020

Annual FISMA Report

Environmental Protection Agency



Function 1: Identify - Risk Management

1 To what extent does the organization maintain a comprehensive and accurate inventory of its information systems (including cloud systems, public facing websites, and third party systems), and system interconnections (NIST SP 800-53. Rev. 4: CA-3, PM-5, and CM-8; NIST 800-161; NIST Cybersecurity Framework (CSF): ID.AM-1 - 4; FY 2020 CIO FISMA Metrics: 1.1 and 1.4, OMB A-130).

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

2 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of hardware assets (including GFE and Bring Your Own Device (BYOD) mobile devices) connected to the organization's network with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7 and CM-8; NIST SP 800-137; NISTIR 8011; Federal Enterprise Architecture (FEA) Framework, v2; FY 2020 CIO FISMA Metrics: 1.2

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

3 To what extent does the organization use standard data elements/taxonomy to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting (NIST SP 800-53 Rev. 4: CA-7, CM-8, and CM-10; NIST SP 800-137; NISTIR 8011; FEA Framework, v2; FY 2020 CIO FISMA Metrics: 1.2.5, 1.3.3, 3.10; CSF: ID.AM-2)?

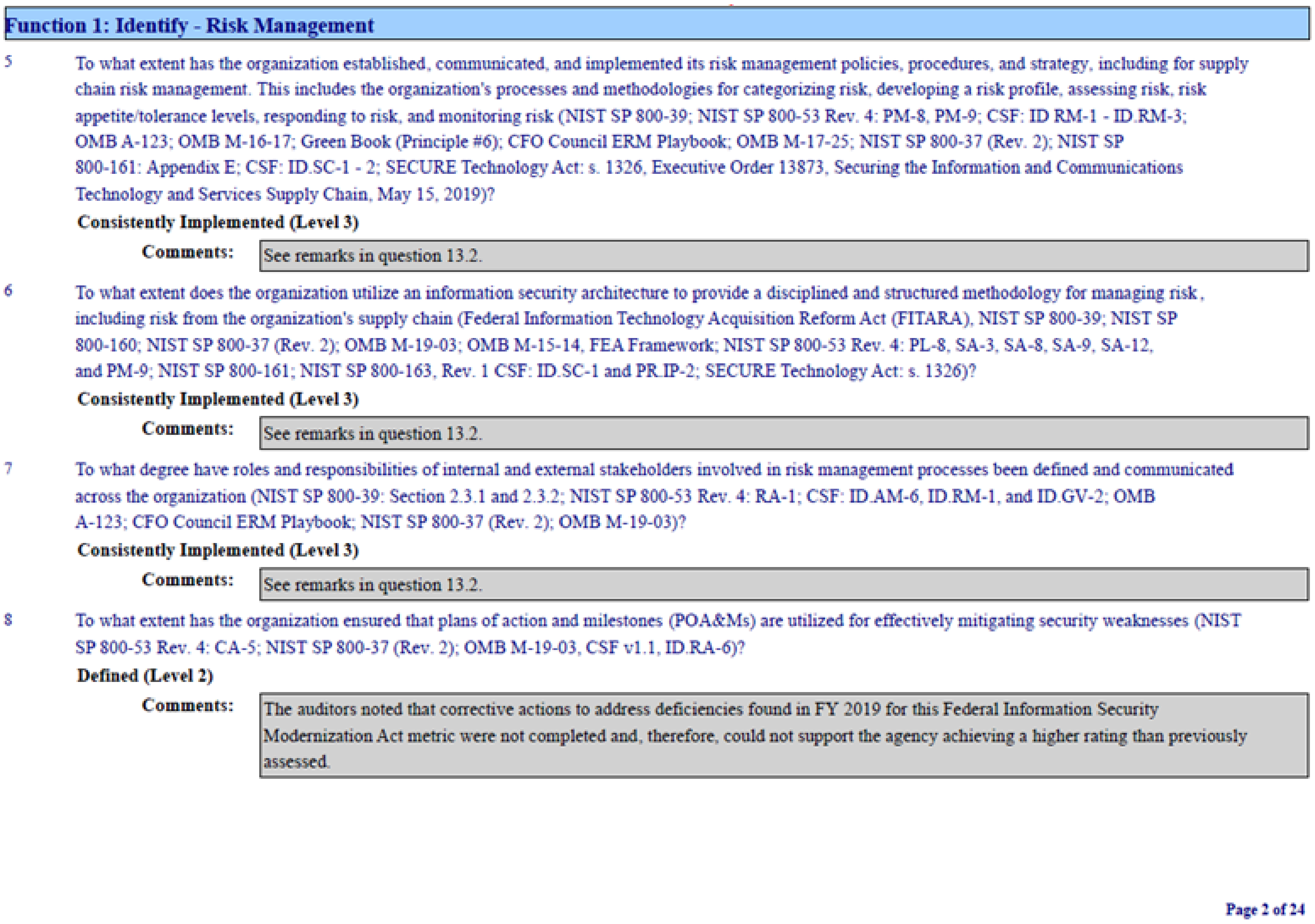
Defined (Level 2)

Comments: The auditors noted that corrective actions to address deficiencies found in fiscal year 2019 for this Federal Information Security Modernization Act metric were not completed and, therefore, could not support the agency achieving a higher rating than previously assessed.

4 To what extent has the organization categorized and communicated the importance/priority of information systems in enabling its missions and business functions, including for high value assets (NIST SP 800-53 Rev. 4: RA-2, PM-7, and PM-11; NIST SP 800-60; NIST SP 800-37 (Rev. 2); CSF: ID.BE-3, ID.AM-5, and ID.SC-2; FIPS 199; FY 2020 CIO FISMA Metrics: 1.1; OMB M-19-03)?

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.



Function 1: Identify - Risk Management

5 To what extent has the organization established, communicated, and implemented its risk management policies, procedures, and strategy, including for supply chain risk management. This includes the organization's processes and methodologies for categorizing risk, developing a risk profile, assessing risk, risk appetite/tolerance levels, responding to risk, and monitoring risk (NIST SP 800-39; NIST SP 800-53 Rev. 4: PM-8, PM-9; CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); CFO Council ERM Playbook; OMB M-17-25; NIST SP 800-37 (Rev. 2); NIST SP 800-161: Appendix E; CSF: ID.SC-1 - 2; SECURE Technology Act: s. 1326, Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019)?

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

6 To what extent does the organization utilize an information security architecture to provide a disciplined and structured methodology for managing risk , including risk from the organization's supply chain (Federal Information Technology Acquisition Reform Act (FITARA), NIST SP 800-39; NIST SP 800-160; NIST SP 800-37 (Rev. 2); OMB M-19-03; OMB M-15-14, FEA Framework; NIST SP 800-53 Rev. 4: PL-8, SA-3, SA-8, SA-9, SA-12, and PM-9; NIST SP 800-161; NIST SP 800-163, Rev. 1 CSF: ID.SC-1 and PR.IP-2; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

7 To what degree have roles and responsibilities of internal and external stakeholders involved in risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1 and 2.3.2; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; OMB A-123; CFO Council ERM Playbook; NIST SP 800-37 (Rev. 2); OMB M-19-03)?

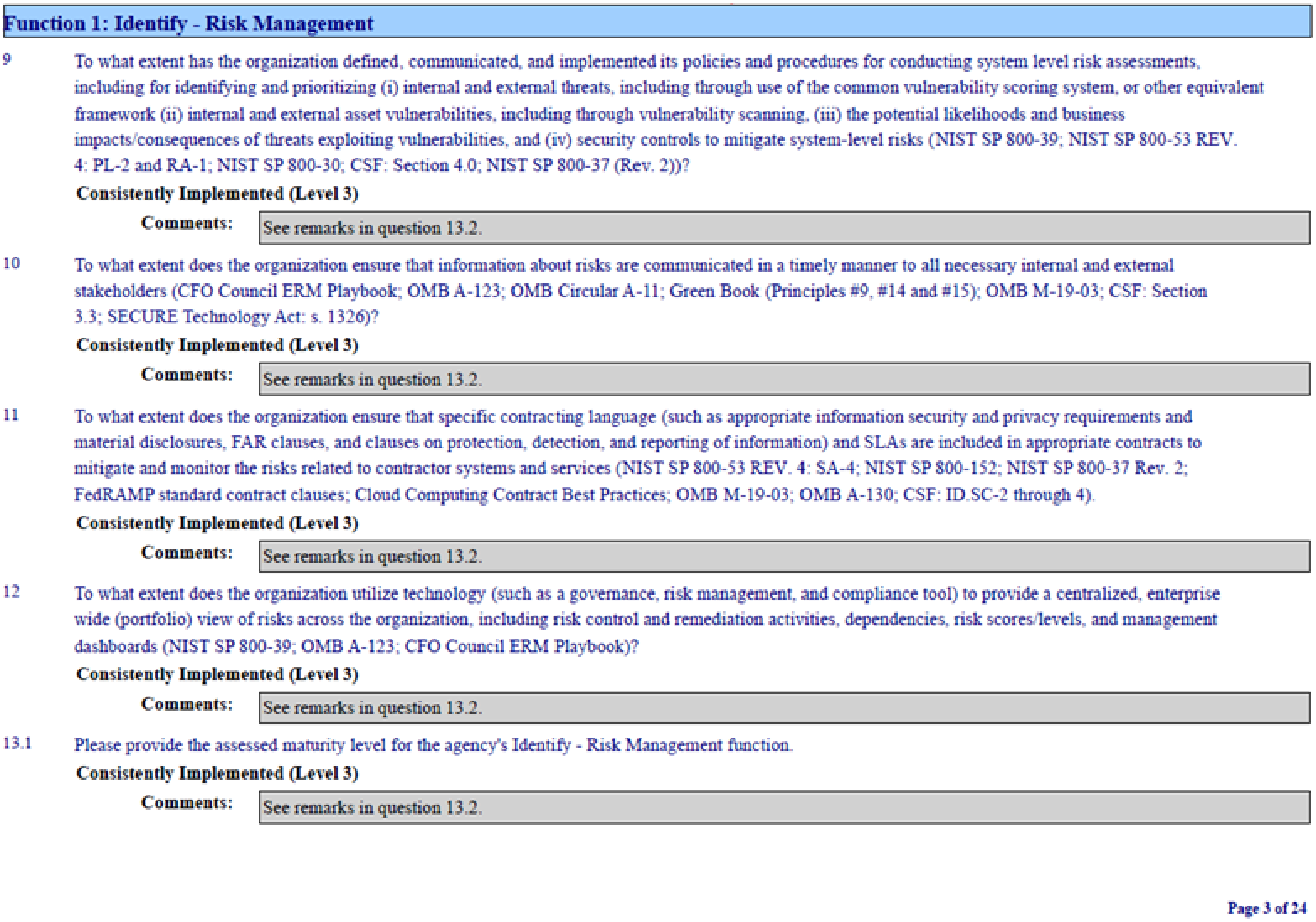
Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

8 To what extent has the organization ensured that plans of action and milestones (POA&Ms) are utilized for effectively mitigating security weaknesses (NIST SP 800-53 Rev. 4: CA-5; NIST SP 800-37 (Rev. 2); OMB M-19-03, CSF v1.1, ID.RA-6)?

Defined (Level 2)

Comments: The auditors noted that corrective actions to address deficiencies found in FY 2019 for this Federal Information Security Modernization Act metric were not completed and, therefore, could not support the agency achieving a higher rating than previously assessed.



Function 1: Identify - Risk Management

9 To what extent has the organization defined, communicated, and implemented its policies and procedures for conducting system level risk assessments, including for identifying and prioritizing (i) internal and external threats, including through use of the common vulnerability scoring system, or other equivalent framework (ii) internal and external asset vulnerabilities, including through vulnerability scanning, (iii) the potential likelihoods and business impacts/consequences of threats exploiting vulnerabilities, and (iv) security controls to mitigate system-level risks (NIST SP 800-39; NIST SP 800-53 REV. 4: PL-2 and RA-1; NIST SP 800-30; CSF: Section 4.0; NIST SP 800-37 (Rev. 2))?

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

10 To what extent does the organization ensure that information about risks are communicated in a timely manner to all necessary internal and external stakeholders (CFO Council ERM Playbook; OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; SECURE Technology Act: s. 1326)?

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

11 To what extent does the organization ensure that specific contracting language (such as appropriate information security and privacy requirements and material disclosures, FAR clauses, and clauses on protection, detection, and reporting of information) and SLAs are included in appropriate contracts to mitigate and monitor the risks related to contractor systems and services (NIST SP 800-53 REV. 4: SA-4; NIST SP 800-152; NIST SP 800-37 Rev. 2; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

12 To what extent does the organization utilize technology (such as a governance, risk management, and compliance tool) to provide a centralized, enterprise wide (portfolio) view of risks across the organization, including risk control and remediation activities, dependencies, risk scores/levels, and management dashboards (NIST SP 800-39; OMB A-123; CFO Council ERM Playbook)?

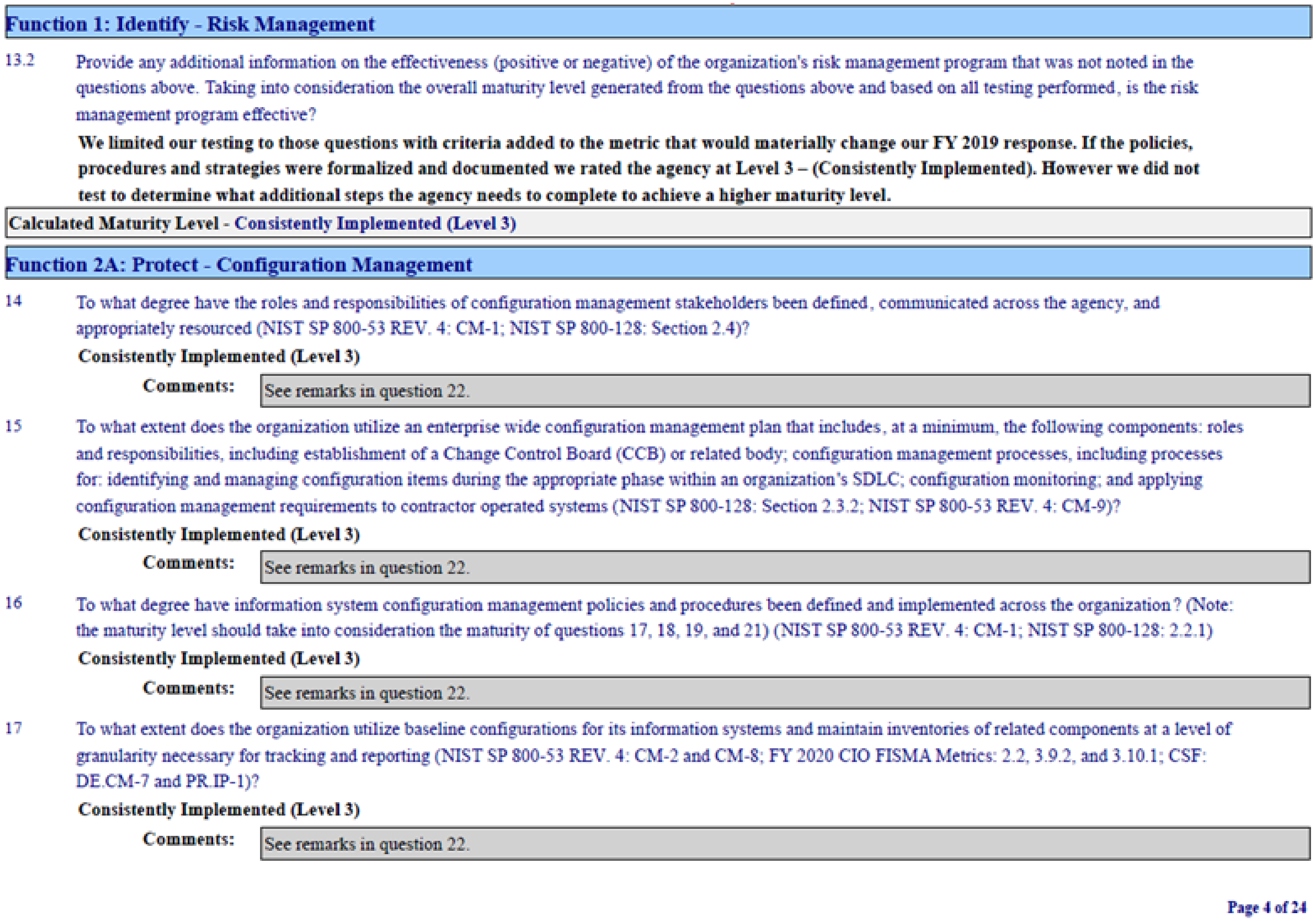
Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.

13.1 Please provide the assessed maturity level for the agency's Identify - Risk Management function.

Consistently Implemented (Level 3)

Comments: See remarks in question 13.2.



Function 1: Identify - Risk Management

13.2 Provide any additional information on the effectiveness (positive or negative) of the organization's risk management program that was not noted in the questions above. Taking into consideration the overall maturity level generated from the questions above and based on all testing performed, is the risk management program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2A: Protect - Configuration Management

14 To what degree have the roles and responsibilities of configuration management stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: Section 2.4)?

Consistently Implemented (Level 3)

Comments: See remarks in question 22.

15 To what extent does the organization utilize an enterprise wide configuration management plan that includes, at a minimum, the following components: roles and responsibilities, including establishment of a Change Control Board (CCB) or related body; configuration management processes, including processes for: identifying and managing configuration items during the appropriate phase within an organization's SDLC; configuration monitoring; and applying configuration management requirements to contractor operated systems (NIST SP 800-128: Section 2.3.2; NIST SP 800-53 REV. 4: CM-9)?

Consistently Implemented (Level 3)

Comments: See remarks in question 22.

16 To what degree have information system configuration management policies and procedures been defined and implemented across the organization? (Note: the maturity level should take into consideration the maturity of questions 17, 18, 19, and 21) (NIST SP 800-53 REV. 4: CM-1; NIST SP 800-128: 2.2.1)

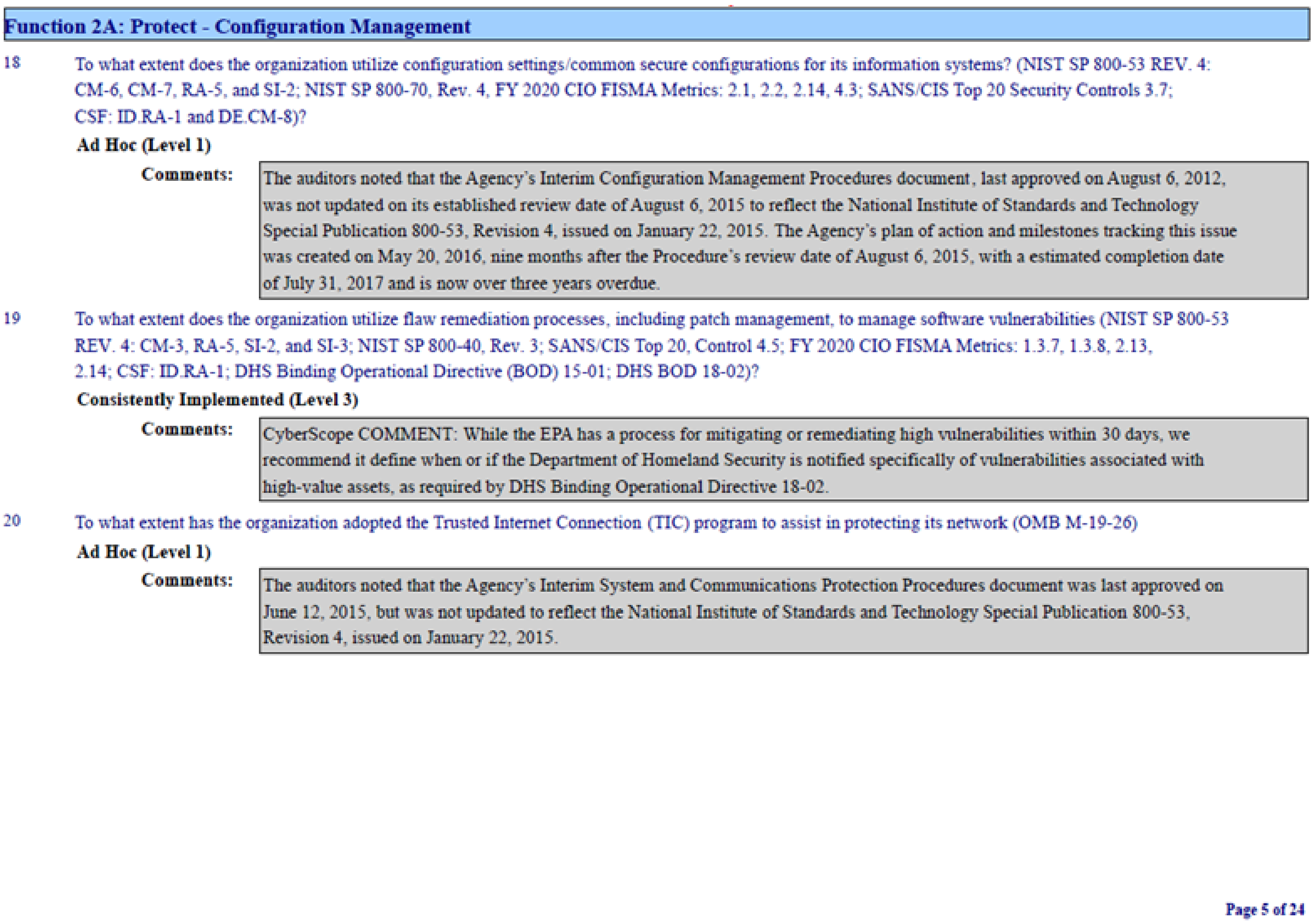
Consistently Implemented (Level 3)

Comments: See remarks in question 22.

17 To what extent does the organization utilize baseline configurations for its information systems and maintain inventories of related components at a level of granularity necessary for tracking and reporting (NIST SP 800-53 REV. 4: CM-2 and CM-8; FY 2020 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

Consistently Implemented (Level 3)

Comments: See remarks in question 22.



Function 2A: Protect - Configuration Management

18 To what extent does the organization utilize configuration settings/common secure configurations for its information systems? (NIST SP 800-53 REV. 4: CM-6, CM-7, RA-5, and SI-2; NIST SP 800-70, Rev. 4, FY 2020 CIO FISMA Metrics: 2.1, 2.2, 2.14, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

Ad Hoc (Level 1)

Comments: The auditors noted that the Agency's Interim Configuration Management Procedures document, last approved on August 6, 2012, was not updated on its established review date of August 6, 2015 to reflect the National Institute of Standards and Technology Special Publication 800-53, Revision 4, issued on January 22, 2015. The Agency's plan of action and milestones tracking this issue was created on May 20, 2016, nine months after the Procedure's review date of August 6, 2015, with a estimated completion date of July 31, 2017 and is now over three years overdue.

19 To what extent does the organization utilize flaw remediation processes, including patch management, to manage software vulnerabilities (NIST SP 800-53 REV. 4: CM-3, RA-5, SI-2, and SI-3; NIST SP 800-40, Rev. 3; SANS/CIS Top 20, Control 4.5; FY 2020 CIO FISMA Metrics: 1.3.7, 1.3.8, 2.13, 2.14; CSF: ID.RA-1; DHS Binding Operational Directive (BOD) 15-01; DHS BOD 18-02)?

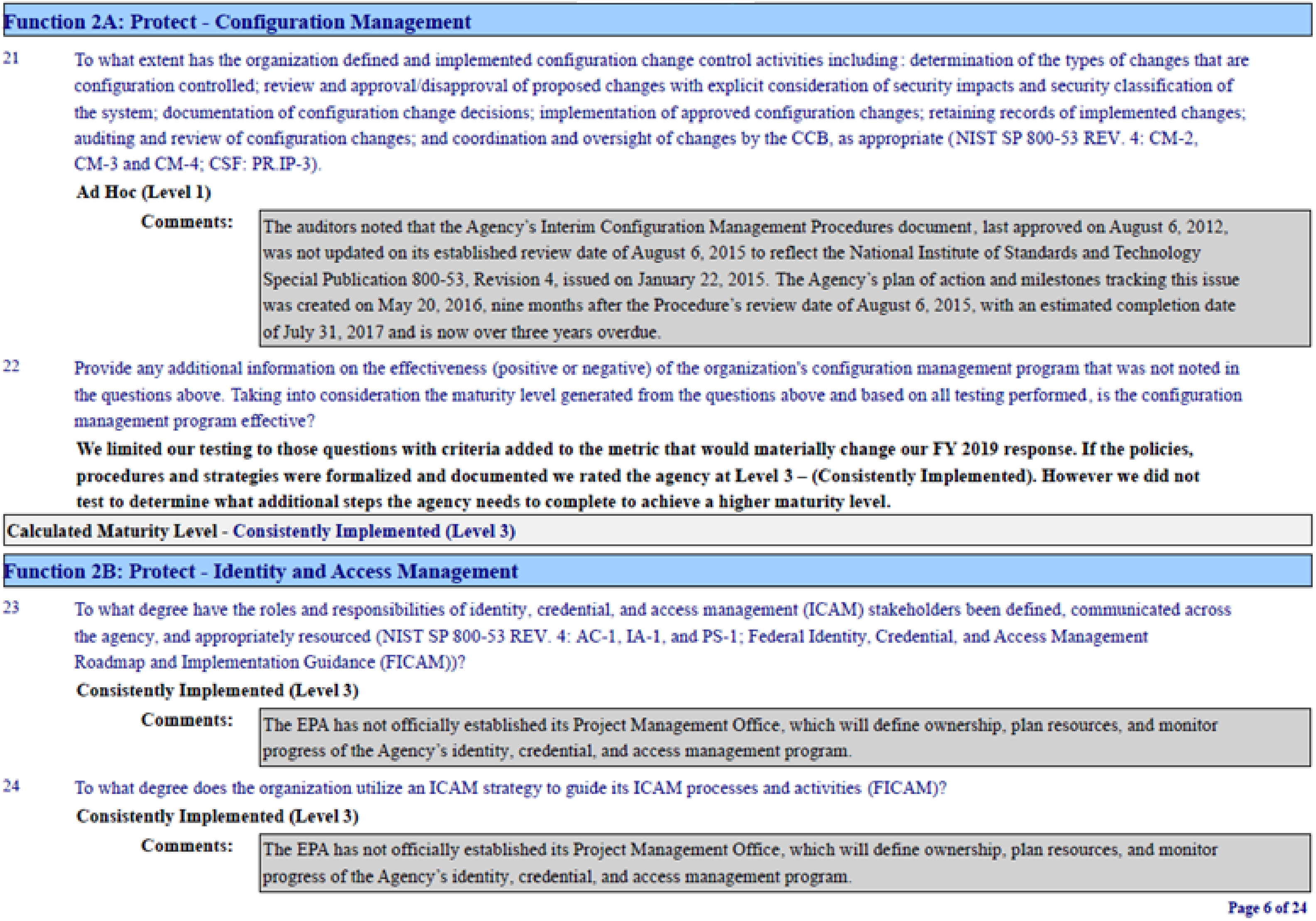
Consistently Implemented (Level 3)

Comments: CyberScope COMMENT: While the EPA has a process for mitigating or remediating high vulnerabilities within 30 days, we recommend it define when or if the Department of Homeland Security is notified specifically of vulnerabilities associated with high-value assets, as required by DHS Binding Operational Directive 18-02.

20 To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)

Ad Hoc (Level 1)

Comments: The auditors noted that the Agency's Interim System and Communications Protection Procedures document was last approved on June 12, 2015, but was not updated to reflect the National Institute of Standards and Technology Special Publication 800-53, Revision 4, issued on January 22, 2015.



Function 2A: Protect - Configuration Management

21 To what extent has the organization defined and implemented configuration change control activities including: determination of the types of changes that are configuration controlled; review and approval/disapproval of proposed changes with explicit consideration of security impacts and security classification of the system; documentation of configuration change decisions; implementation of approved configuration changes; retaining records of implemented changes; auditing and review of configuration changes; and coordination and oversight of changes by the CCB, as appropriate (NIST SP 800-53 REV. 4: CM-2, CM-3 and CM-4; CSF: PR.IP-3).

Ad Hoc (Level 1)

Comments: The auditors noted that the Agency's Interim Configuration Management Procedures document, last approved on August 6, 2012, was not updated on its established review date of August 6, 2015 to reflect the National Institute of Standards and Technology Special Publication 800-53, Revision 4, issued on January 22, 2015. The Agency's plan of action and milestones tracking this issue was created on May 20, 2016, nine months after the Procedure's review date of August 6, 2015, with an estimated completion date of July 31, 2017 and is now over three years overdue.

22 Provide any additional information on the effectiveness (positive or negative) of the organization's configuration management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the configuration management program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2B: Protect - Identity and Access Management

23 To what degree have the roles and responsibilities of identity, credential, and access management (ICAM) stakeholders been defined, communicated across the agency, and appropriately resourced (NIST SP 800-53 REV. 4: AC-1, IA-1, and PS-1; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM))?

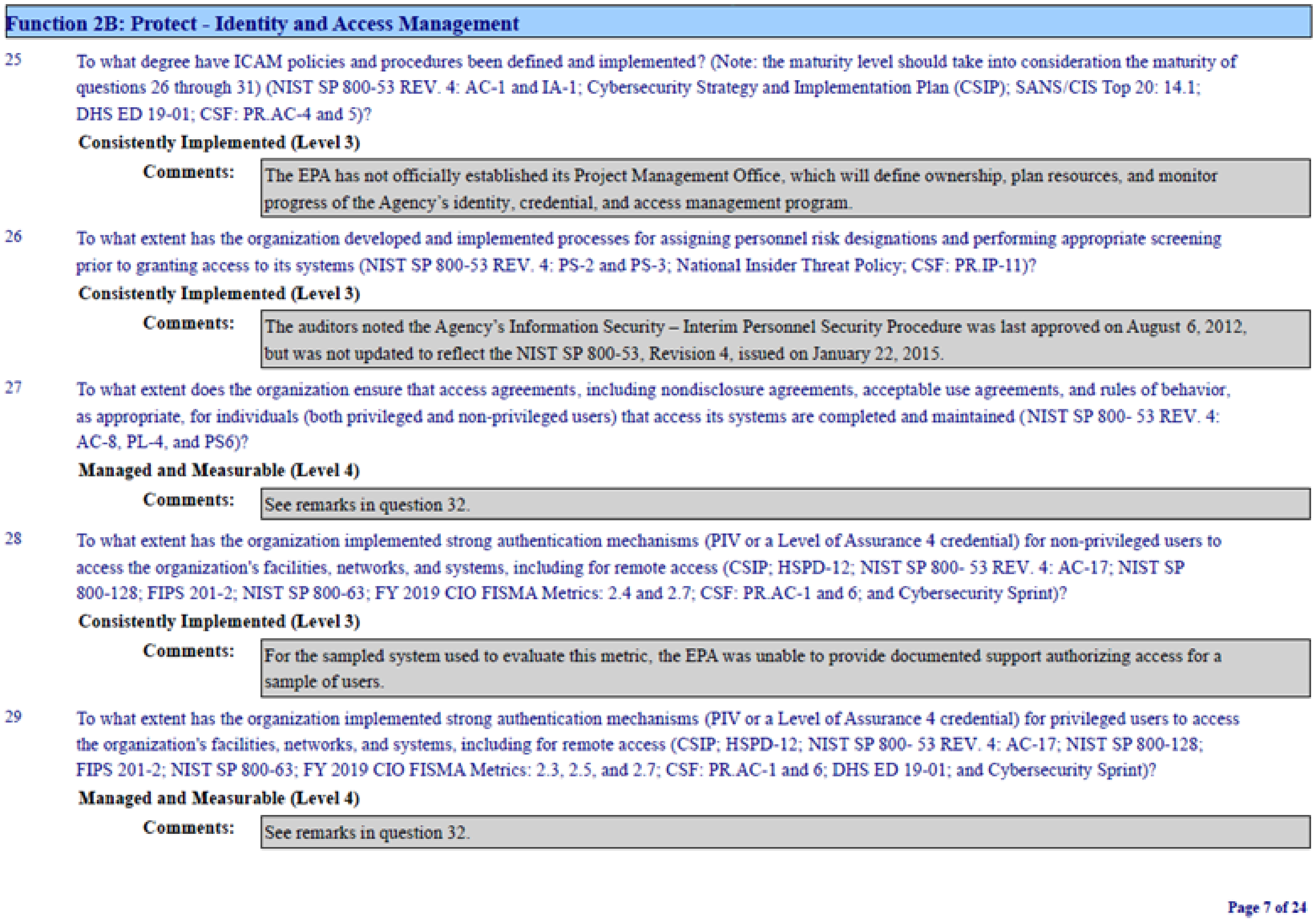
Consistently Implemented (Level 3)

Comments: The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program.

24 To what degree does the organization utilize an ICAM strategy to guide its ICAM processes and activities (FICAM)?

Consistently Implemented (Level 3)

Comments: The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program.



Function 2B: Protect - Identity and Access Management

25 To what degree have ICAM policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 26 through 31) (NIST SP 800-53 REV. 4: AC-1 and IA-1; Cybersecurity Strategy and Implementation Plan (CSIP); SANS/CIS Top 20: 14.1; DHS ED 19-01; CSF: PR.AC-4 and 5)?

Consistently Implemented (Level 3)

Comments: The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program.

26 To what extent has the organization developed and implemented processes for assigning personnel risk designations and performing appropriate screening prior to granting access to its systems (NIST SP 800-53 REV. 4: PS-2 and PS-3; National Insider Threat Policy; CSF: PR.IP-11)?

Consistently Implemented (Level 3)

Comments: The auditors noted the Agency's Information Security – Interim Personnel Security Procedure was last approved on August 6, 2012, but was not updated to reflect the NIST SP 800-53, Revision 4, issued on January 22, 2015.

27 To what extent does the organization ensure that access agreements, including nondisclosure agreements, acceptable use agreements, and rules of behavior, as appropriate, for individuals (both privileged and non-privileged users) that access its systems are completed and maintained (NIST SP 800- 53 REV. 4: AC-8, PL-4, and PS6)?

Managed and Measurable (Level 4)

Comments: See remarks in question 32.

28 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for non-privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.4 and 2.7; CSF: PR.AC-1 and 6; and Cybersecurity Sprint)?

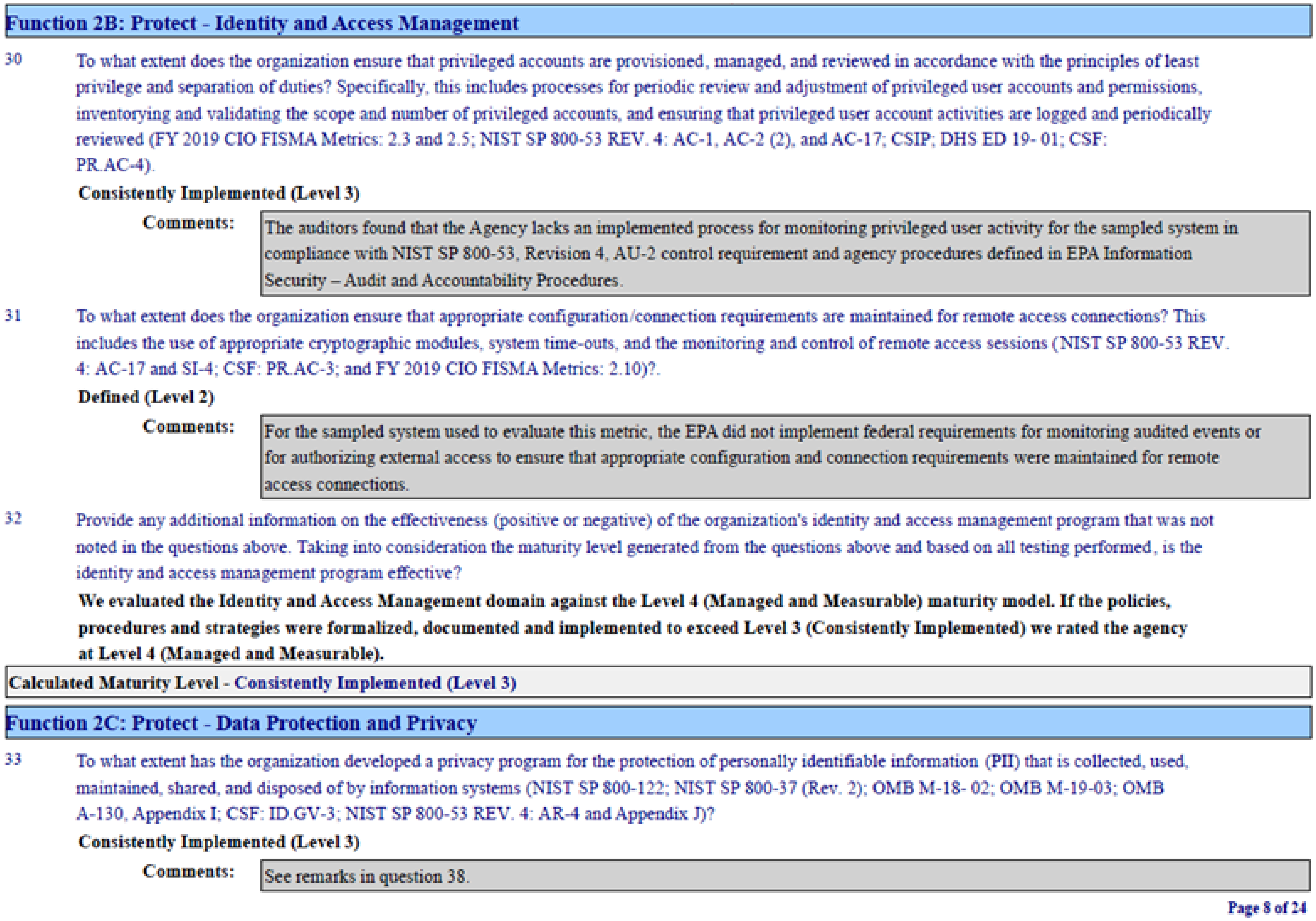
Consistently Implemented (Level 3)

Comments: For the sampled system used to evaluate this metric, the EPA was unable to provide documented support authorizing access for a sample of users.

29 To what extent has the organization implemented strong authentication mechanisms (PIV or a Level of Assurance 4 credential) for privileged users to access the organization's facilities, networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800- 53 REV. 4: AC-17; NIST SP 800-128; FIPS 201-2; NIST SP 800-63; FY 2019 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; DHS ED 19-01; and Cybersecurity Sprint)?

Managed and Measurable (Level 4)

Comments: See remarks in question 32.



Function 2B: Protect - Identity and Access Management

30 To what extent does the organization ensure that privileged accounts are provisioned, managed, and reviewed in accordance with the principles of least privilege and separation of duties? Specifically, this includes processes for periodic review and adjustment of privileged user accounts and permissions, inventorying and validating the scope and number of privileged accounts, and ensuring that privileged user account activities are logged and periodically reviewed (FY 2019 CIO FISMA Metrics: 2.3 and 2.5; NIST SP 800-53 REV. 4: AC-1, AC-2 (2), and AC-17; CSIP; DHS ED 19- 01; CSF: PR.AC-4).

Consistently Implemented (Level 3)

Comments: The auditors found that the Agency lacks an implemented process for monitoring privileged user activity for the sampled system in compliance with NIST SP 800-53, Revision 4, AU-2 control requirement and agency procedures defined in EPA Information Security – Audit and Accountability Procedures.

31 To what extent does the organization ensure that appropriate configuration/connection requirements are maintained for remote access connections? This includes the use of appropriate cryptographic modules, system time-outs, and the monitoring and control of remote access sessions (NIST SP 800-53 REV. 4: AC-17 and SI-4; CSF: PR.AC-3; and FY 2019 CIO FISMA Metrics: 2.10)?.

Defined (Level 2)

Comments: For the sampled system used to evaluate this metric, the EPA did not implement federal requirements for monitoring audited events or for authorizing external access to ensure that appropriate configuration and connection requirements were maintained for remote access connections.

32 Provide any additional information on the effectiveness (positive or negative) of the organization's identity and access management program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the identity and access management program effective?

We evaluated the Identity and Access Management domain against the Level 4 (Managed and Measurable) maturity model. If the policies, procedures and strategies were formalized, documented and implemented to exceed Level 3 (Consistently Implemented) we rated the agency at Level 4 (Managed and Measurable).

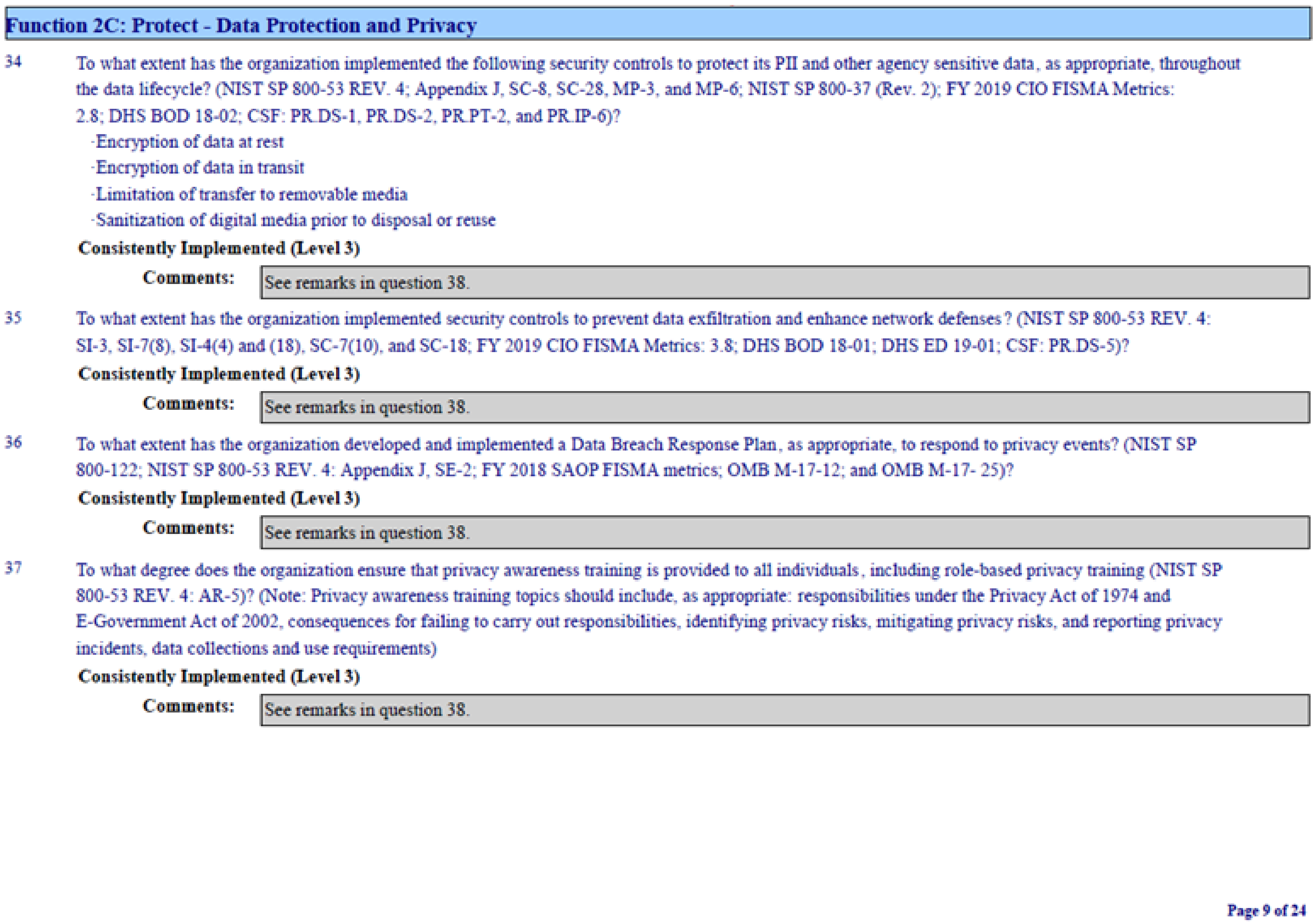
Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2C: Protect - Data Protection and Privacy

33 To what extent has the organization developed a privacy program for the protection of personally identifiable information (PII) that is collected, used, maintained, shared, and disposed of by information systems (NIST SP 800-122; NIST SP 800-37 (Rev. 2); OMB M-18- 02; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J)?

Consistently Implemented (Level 3)

Comments: See remarks in question 38.



Function 2C: Protect - Data Protection and Privacy

34 To what extent has the organization implemented the following security controls to protect its PII and other agency sensitive data, as appropriate, throughout the data lifecycle? (NIST SP 800-53 REV. 4; Appendix J, SC-8, SC-28, MP-3, and MP-6; NIST SP 800-37 (Rev. 2); FY 2019 CIO FISMA Metrics: 2.8; DHS BOD 18-02; CSF: PR.DS-1, PR.DS-2, PR.PT-2, and PR.IP-6)?

-Encryption of data at rest
-Encryption of data in transit
-Limitation of transfer to removable media
-Sanitization of digital media prior to disposal or reuse

Consistently Implemented (Level 3)

Comments: See remarks in question 38.

35 To what extent has the organization implemented security controls to prevent data exfiltration and enhance network defenses? (NIST SP 800-53 REV. 4: SI-3, SI-7(8), SI-4(4) and (18), SC-7(10), and SC-18; FY 2019 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Consistently Implemented (Level 3)

Comments: See remarks in question 38.

36 To what extent has the organization developed and implemented a Data Breach Response Plan, as appropriate, to respond to privacy events? (NIST SP 800-122; NIST SP 800-53 REV. 4: Appendix J, SE-2; FY 2018 SAOP FISMA metrics; OMB M-17-12; and OMB M-17- 25)?

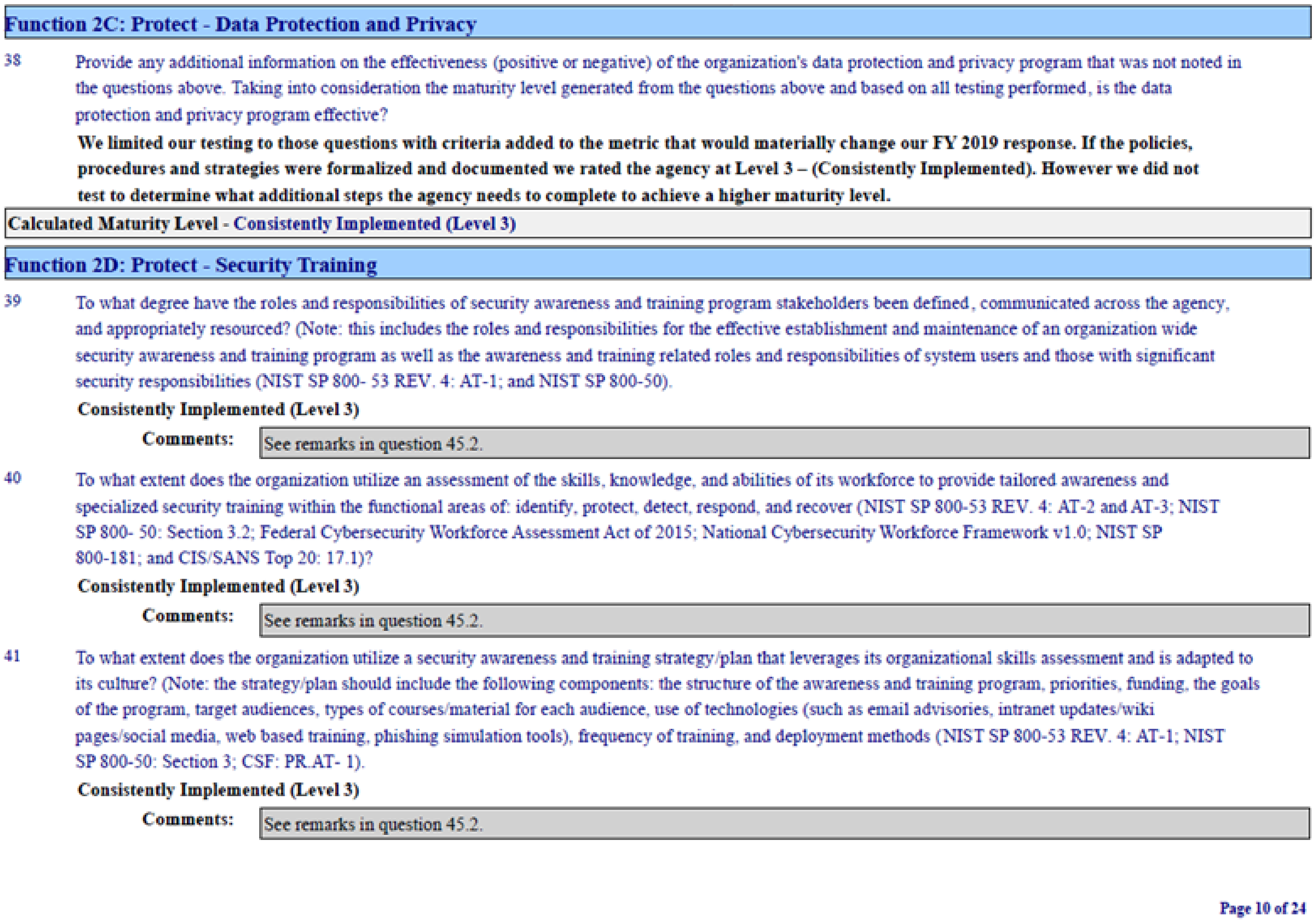
Consistently Implemented (Level 3)

Comments: See remarks in question 38.

37 To what degree does the organization ensure that privacy awareness training is provided to all individuals, including role-based privacy training (NIST SP 800-53 REV. 4: AR-5)? (Note: Privacy awareness training topics should include, as appropriate: responsibilities under the Privacy Act of 1974 and E-Government Act of 2002, consequences for failing to carry out responsibilities, identifying privacy risks, mitigating privacy risks, and reporting privacy incidents, data collections and use requirements)

Consistently Implemented (Level 3)

Comments: See remarks in question 38.



Function 2C: Protect - Data Protection and Privacy

38 Provide any additional information on the effectiveness (positive or negative) of the organization's data protection and privacy program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the data protection and privacy program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 2D: Protect - Security Training

39 To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, communicated across the agency, and appropriately resourced? (Note: this includes the roles and responsibilities for the effective establishment and maintenance of an organization wide security awareness and training program as well as the awareness and training related roles and responsibilities of system users and those with significant security responsibilities (NIST SP 800- 53 REV. 4: AT-1; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.

40 To what extent does the organization utilize an assessment of the skills, knowledge, and abilities of its workforce to provide tailored awareness and specialized security training within the functional areas of: identify, protect, detect, respond, and recover (NIST SP 800-53 REV. 4: AT-2 and AT-3; NIST SP 800- 50: Section 3.2; Federal Cybersecurity Workforce Assessment Act of 2015; National Cybersecurity Workforce Framework v1.0; NIST SP 800-181; and CIS/SANS Top 20: 17.1)?

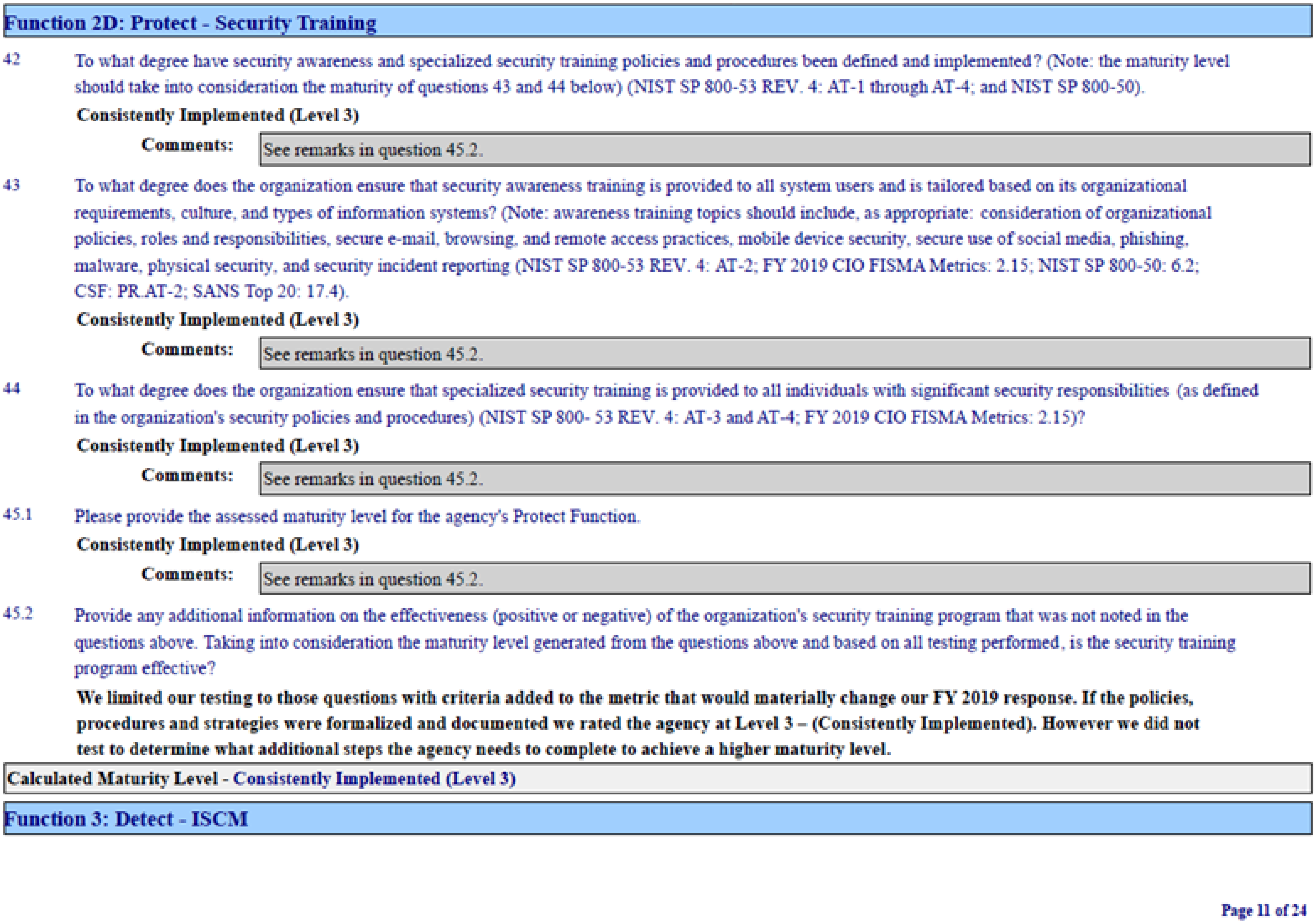
Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.

41 To what extent does the organization utilize a security awareness and training strategy/plan that leverages its organizational skills assessment and is adapted to its culture? (Note: the strategy/plan should include the following components: the structure of the awareness and training program, priorities, funding, the goals of the program, target audiences, types of courses/material for each audience, use of technologies (such as email advisories, intranet updates/wiki pages/social media, web based training, phishing simulation tools), frequency of training, and deployment methods (NIST SP 800-53 REV. 4: AT-1; NIST SP 800-50: Section 3; CSF: PR.AT- 1).

Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.



Function 2D: Protect - Security Training

42 To what degree have security awareness and specialized security training policies and procedures been defined and implemented? (Note: the maturity level should take into consideration the maturity of questions 43 and 44 below) (NIST SP 800-53 REV. 4: AT-1 through AT-4; and NIST SP 800-50).

Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.

43 To what degree does the organization ensure that security awareness training is provided to all system users and is tailored based on its organizational requirements, culture, and types of information systems? (Note: awareness training topics should include, as appropriate: consideration of organizational policies, roles and responsibilities, secure e-mail, browsing, and remote access practices, mobile device security, secure use of social media, phishing, malware, physical security, and security incident reporting (NIST SP 800-53 REV. 4: AT-2; FY 2019 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.

44 To what degree does the organization ensure that specialized security training is provided to all individuals with significant security responsibilities (as defined in the organization's security policies and procedures) (NIST SP 800- 53 REV. 4: AT-3 and AT-4; FY 2019 CIO FISMA Metrics: 2.15)?

Consistently Implemented (Level 3)

Comments: See remarks in question 45.2.

45.1 Please provide the assessed maturity level for the agency's Protect Function.

Consistently Implemented (Level 3)

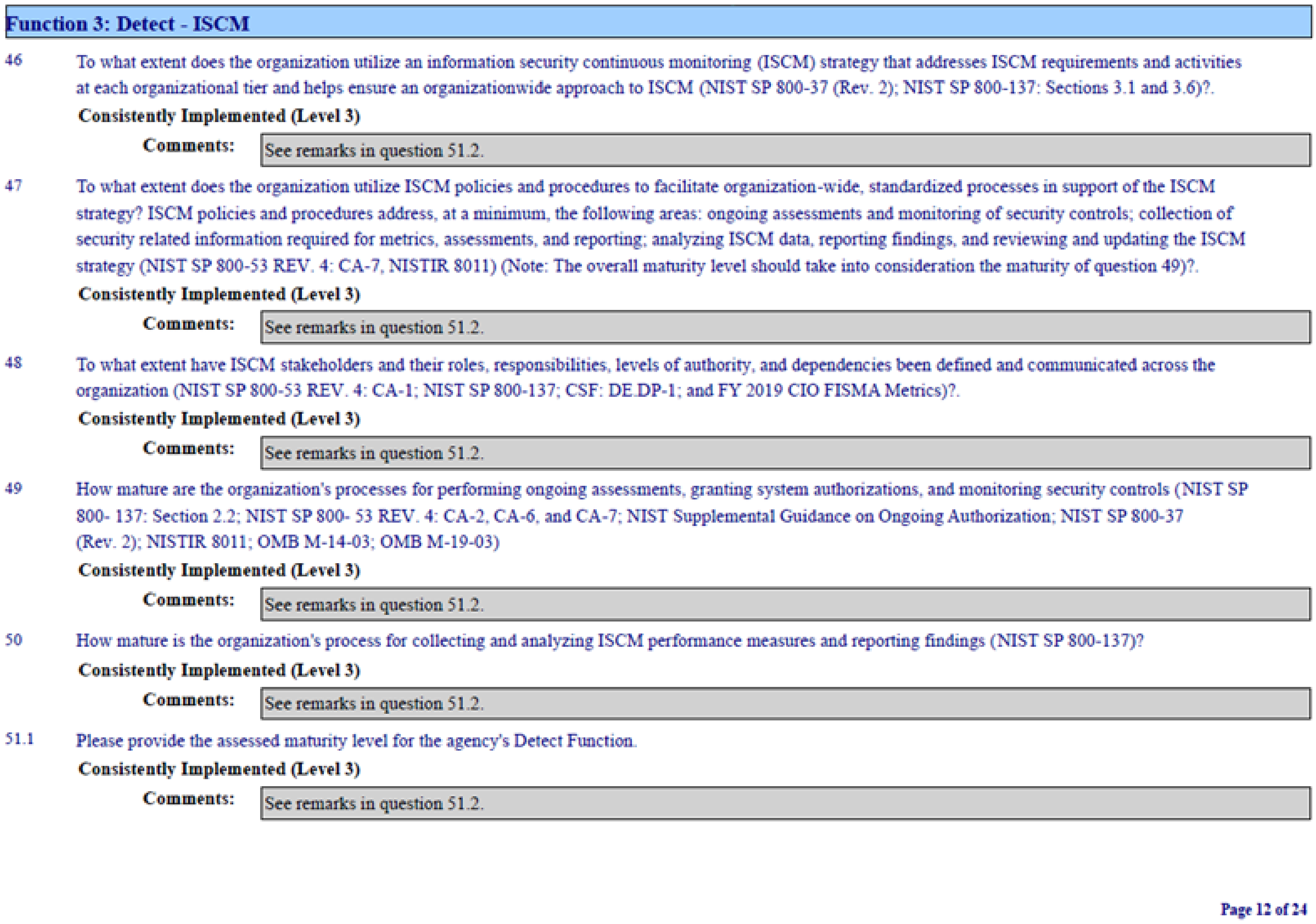
Comments: See remarks in question 45.2.

45.2 Provide any additional information on the effectiveness (positive or negative) of the organization's security training program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the security training program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 3: Detect - ISCM



Function 3: Detect - ISCM

46 To what extent does the organization utilize an information security continuous monitoring (ISCM) strategy that addresses ISCM requirements and activities at each organizational tier and helps ensure an organizationwide approach to ISCM (NIST SP 800-37 (Rev. 2); NIST SP 800-137: Sections 3.1 and 3.6)?.

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

47 To what extent does the organization utilize ISCM policies and procedures to facilitate organization-wide, standardized processes in support of the ISCM strategy? ISCM policies and procedures address, at a minimum, the following areas: ongoing assessments and monitoring of security controls; collection of security related information required for metrics, assessments, and reporting; analyzing ISCM data, reporting findings, and reviewing and updating the ISCM strategy (NIST SP 800-53 REV. 4: CA-7, NISTIR 8011) (Note: The overall maturity level should take into consideration the maturity of question 49)?.

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

48 To what extent have ISCM stakeholders and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: CA-1; NIST SP 800-137; CSF: DE.DP-1; and FY 2019 CIO FISMA Metrics)?.

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

49 How mature are the organization's processes for performing ongoing assessments, granting system authorizations, and monitoring security controls (NIST SP 800- 137: Section 2.2; NIST SP 800- 53 REV. 4: CA-2, CA-6, and CA-7; NIST Supplemental Guidance on Ongoing Authorization; NIST SP 800-37 (Rev. 2); NISTIR 8011; OMB M-14-03; OMB M-19-03)

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

50 How mature is the organization's process for collecting and analyzing ISCM performance measures and reporting findings (NIST SP 800-137)?

Consistently Implemented (Level 3)

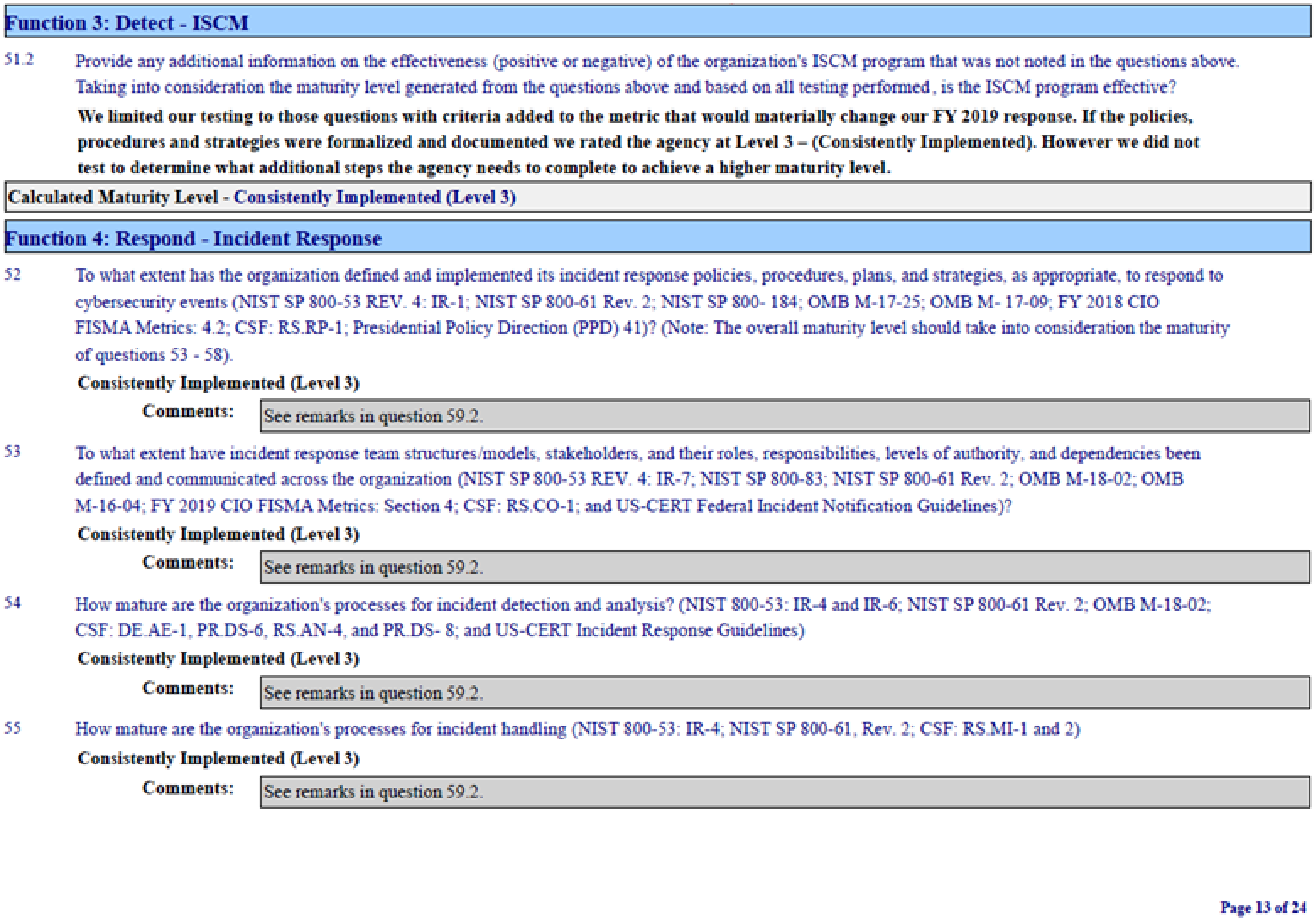
Comments: See remarks in question 51.2.

51.1 Please provide the assessed maturity level for the agency's Detect Function.

Consistently Implemented (Level 3)

Comments: See remarks in question 51.2.

Page 12 of 24



Function 3: Detect - ISCM

51.2 Provide any additional information on the effectiveness (positive or negative) of the organization's ISCM program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the ISCM program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 4: Respond - Incident Response

52 To what extent has the organization defined and implemented its incident response policies, procedures, plans, and strategies, as appropriate, to respond to cybersecurity events (NIST SP 800-53 REV. 4: IR-1; NIST SP 800-61 Rev. 2; NIST SP 800- 184; OMB M-17-25; OMB M- 17-09; FY 2018 CIO FISMA Metrics: 4.2; CSF: RS.RP-1; Presidential Policy Direction (PPD) 41)? (Note: The overall maturity level should take into consideration the maturity of questions 53 - 58).

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

53 To what extent have incident response team structures/models, stakeholders, and their roles, responsibilities, levels of authority, and dependencies been defined and communicated across the organization (NIST SP 800-53 REV. 4: IR-7; NIST SP 800-83; NIST SP 800-61 Rev. 2; OMB M-18-02; OMB M-16-04; FY 2019 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

54 How mature are the organization's processes for incident detection and analysis? (NIST 800-53: IR-4 and IR-6; NIST SP 800-61 Rev. 2; OMB M-18-02; CSF: DE.AE-1, PR.DS-6, RS.AN-4, and PR.DS- 8; and US-CERT Incident Response Guidelines)

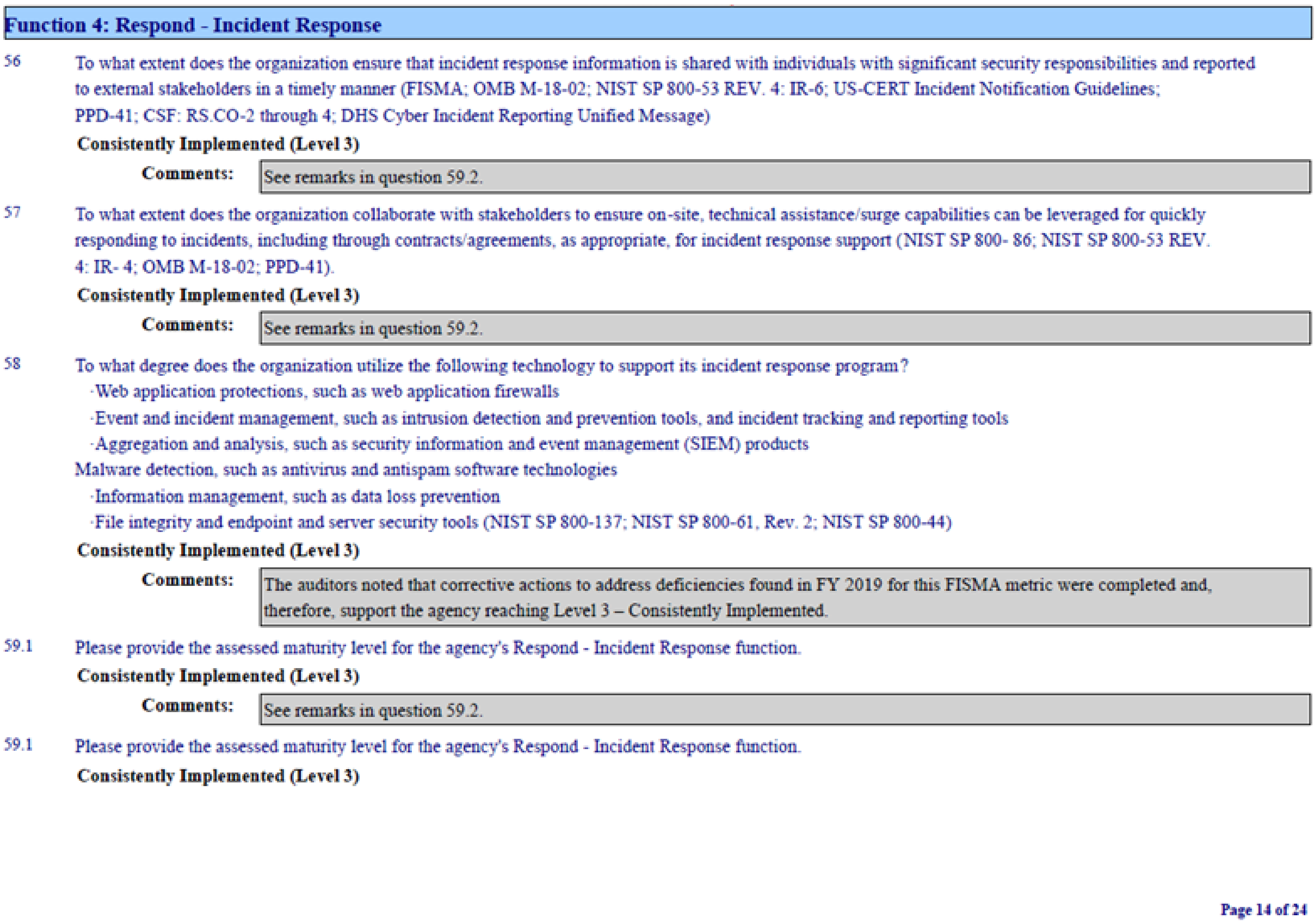
Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

55 How mature are the organization's processes for incident handling (NIST 800-53: IR-4; NIST SP 800-61, Rev. 2; CSF: RS.MI-1 and 2)

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.



Function 4: Respond - Incident Response

56 To what extent does the organization ensure that incident response information is shared with individuals with significant security responsibilities and reported to external stakeholders in a timely manner (FISMA; OMB M-18-02; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 4; DHS Cyber Incident Reporting Unified Message)

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

57 To what extent does the organization collaborate with stakeholders to ensure on-site, technical assistance/surge capabilities can be leveraged for quickly responding to incidents, including through contracts/agreements, as appropriate, for incident response support (NIST SP 800- 86; NIST SP 800-53 REV. 4: IR- 4; OMB M-18-02; PPD-41).

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

58 To what degree does the organization utilize the following technology to support its incident response program?

·Web application protections, such as web application firewalls

·Event and incident management, such as intrusion detection and prevention tools, and incident tracking and reporting tools

·Aggregation and analysis, such as security information and event management (SIEM) products

Malware detection, such as antivirus and antispam software technologies

·Information management, such as data loss prevention

·File integrity and endpoint and server security tools (NIST SP 800-137; NIST SP 800-61, Rev. 2; NIST SP 800-44)

Consistently Implemented (Level 3)

Comments: The auditors noted that corrective actions to address deficiencies found in FY 2019 for this FISMA metric were completed and, therefore, support the agency reaching Level 3 – Consistently Implemented.

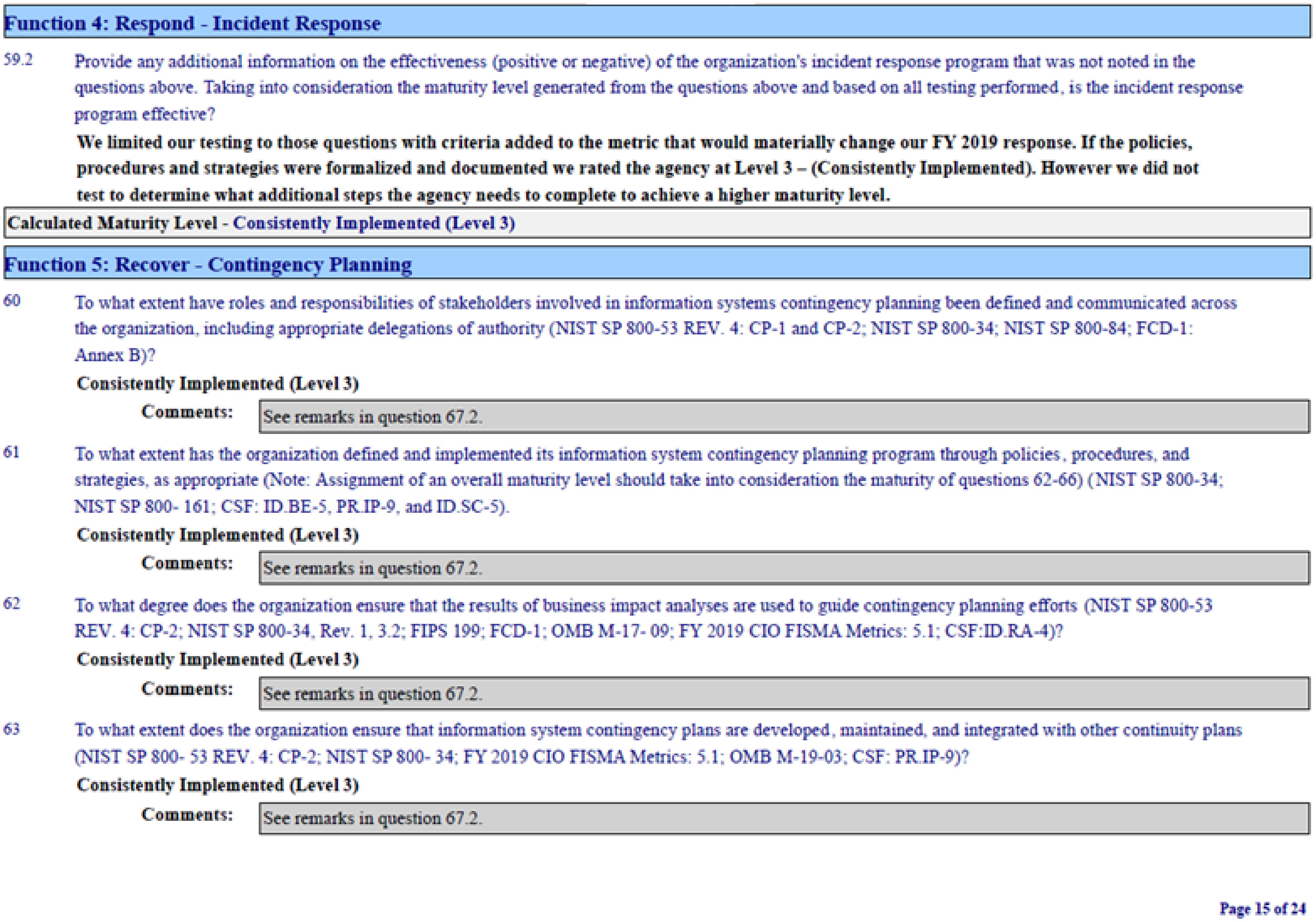
59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Consistently Implemented (Level 3)

Comments: See remarks in question 59.2.

59.1 Please provide the assessed maturity level for the agency's Respond - Incident Response function.

Consistently Implemented (Level 3)



Function 4: Respond - Incident Response

59.2 Provide any additional information on the effectiveness (positive or negative) of the organization's incident response program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the incident response program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 5: Recover - Contingency Planning

60 To what extent have roles and responsibilities of stakeholders involved in information systems contingency planning been defined and communicated across the organization, including appropriate delegations of authority (NIST SP 800-53 REV. 4: CP-1 and CP-2; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

61 To what extent has the organization defined and implemented its information system contingency planning program through policies, procedures, and strategies, as appropriate (Note: Assignment of an overall maturity level should take into consideration the maturity of questions 62-66) (NIST SP 800-34; NIST SP 800- 161; CSF: ID.BE-5, PR.IP-9, and ID.SC-5).

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

62 To what degree does the organization ensure that the results of business impact analyses are used to guide contingency planning efforts (NIST SP 800-53 REV. 4: CP-2; NIST SP 800-34, Rev. 1, 3.2; FIPS 199; FCD-1; OMB M-17- 09; FY 2019 CIO FISMA Metrics: 5.1; CSF:ID.RA-4)?

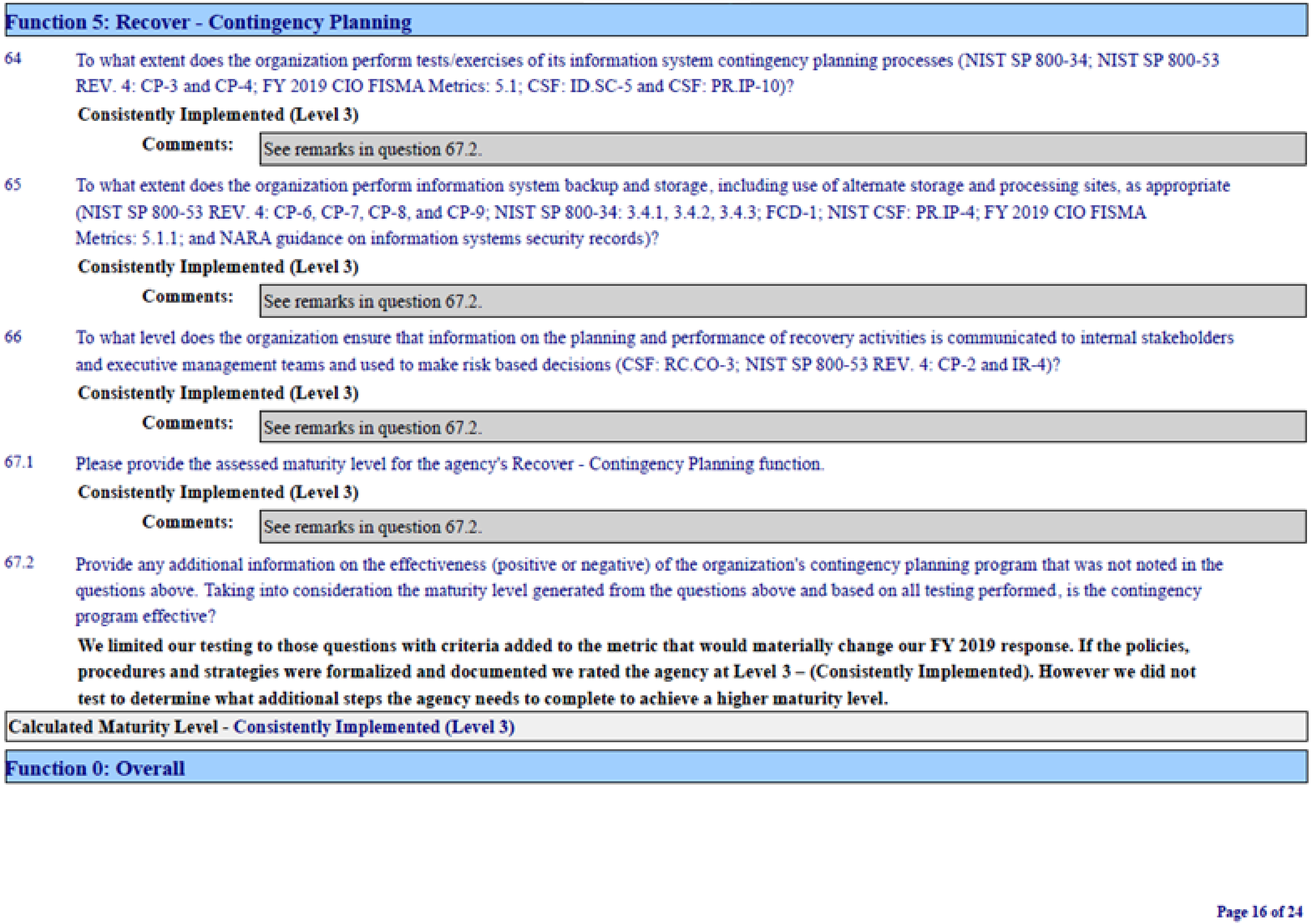
Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

63 To what extent does the organization ensure that information system contingency plans are developed, maintained, and integrated with other continuity plans (NIST SP 800- 53 REV. 4: CP-2; NIST SP 800- 34; FY 2019 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.



Function 5: Recover - Contingency Planning

64 To what extent does the organization perform tests/exercises of its information system contingency planning processes (NIST SP 800-34; NIST SP 800-53 REV. 4: CP-3 and CP-4; FY 2019 CIO FISMA Metrics: 5.1; CSF: ID.SC-5 and CSF: PR.IP-10)?

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

65 To what extent does the organization perform information system backup and storage, including use of alternate storage and processing sites, as appropriate (NIST SP 800-53 REV. 4: CP-6, CP-7, CP-8, and CP-9; NIST SP 800-34: 3.4.1, 3.4.2, 3.4.3; FCD-1; NIST CSF: PR.IP-4; FY 2019 CIO FISMA Metrics: 5.1.1; and NARA guidance on information systems security records)?

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

66 To what level does the organization ensure that information on the planning and performance of recovery activities is communicated to internal stakeholders and executive management teams and used to make risk based decisions (CSF: RC.CO-3; NIST SP 800-53 REV. 4: CP-2 and IR-4)?

Consistently Implemented (Level 3)

Comments: See remarks in question 67.2.

67.1 Please provide the assessed maturity level for the agency's Recover - Contingency Planning function.

Consistently Implemented (Level 3)

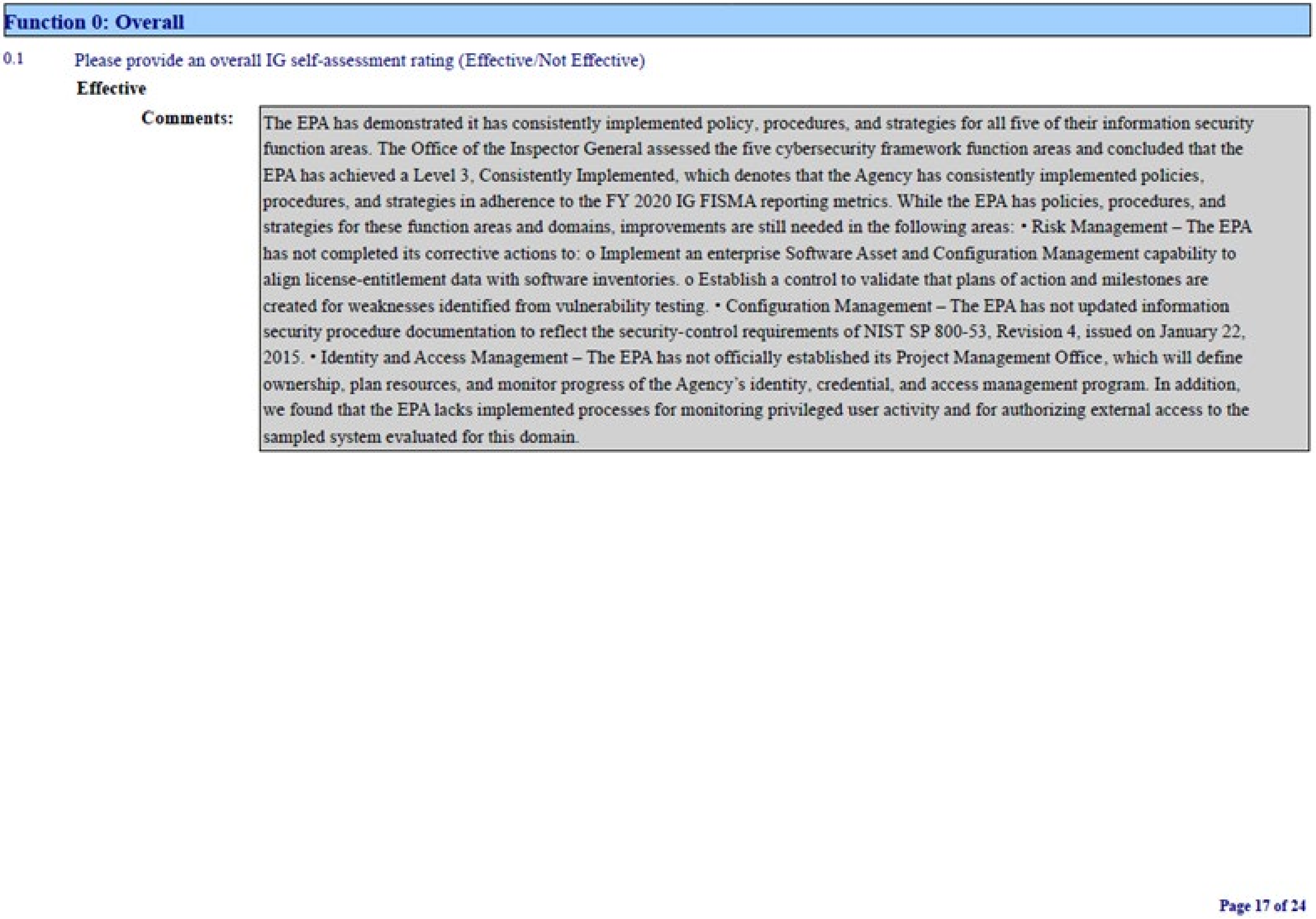
Comments: See remarks in question 67.2.

67.2 Provide any additional information on the effectiveness (positive or negative) of the organization's contingency planning program that was not noted in the questions above. Taking into consideration the maturity level generated from the questions above and based on all testing performed, is the contingency program effective?

We limited our testing to those questions with criteria added to the metric that would materially change our FY 2019 response. If the policies, procedures and strategies were formalized and documented we rated the agency at Level 3 – (Consistently Implemented). However we did not test to determine what additional steps the agency needs to complete to achieve a higher maturity level.

Calculated Maturity Level - Consistently Implemented (Level 3)

Function 0: Overall

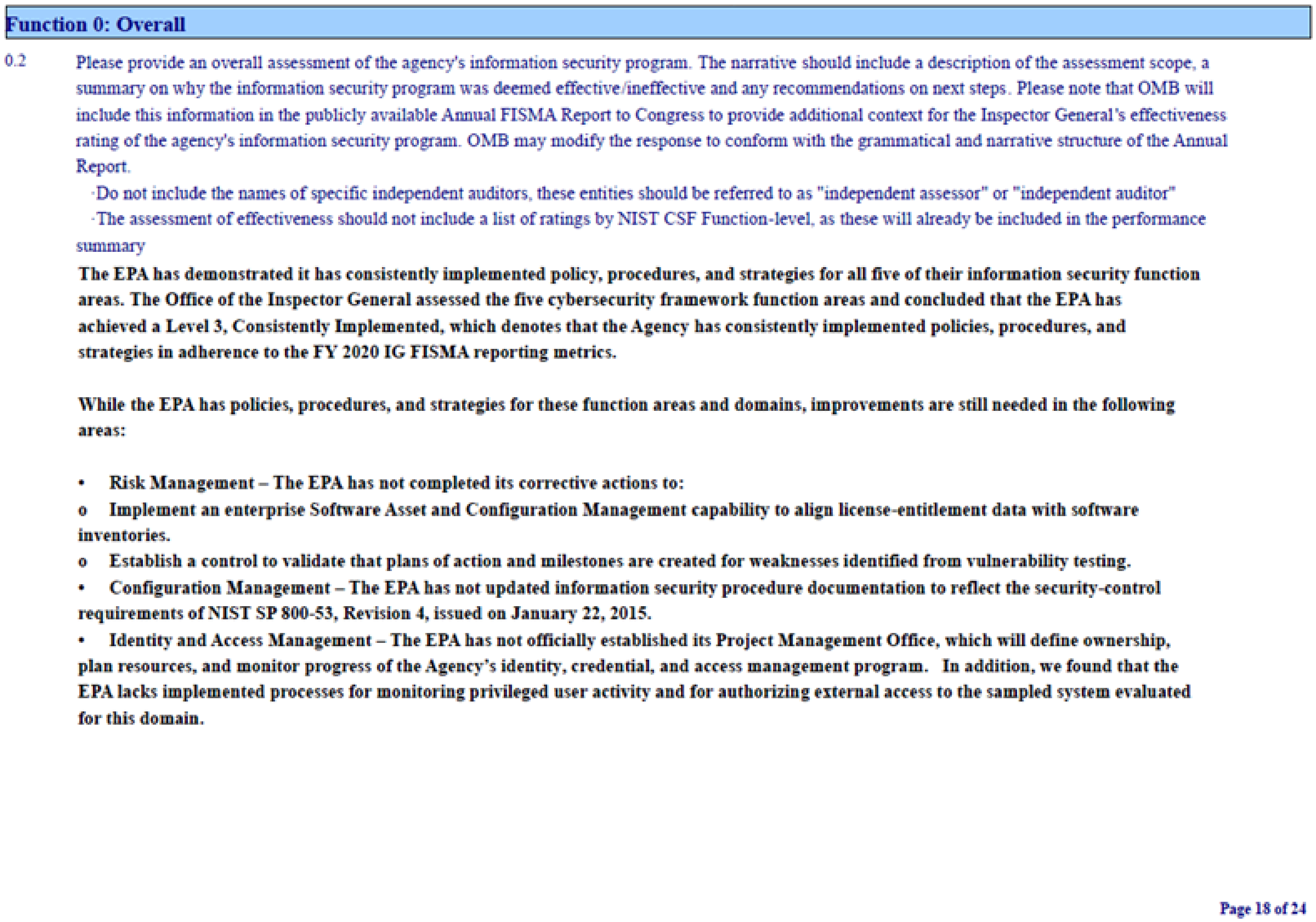


Function 0: Overall

0.1 Please provide an overall IG self-assessment rating (Effective/Not Effective)

Effective

Comments: The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The Office of the Inspector General assessed the five cybersecurity framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2020 IG FISMA reporting metrics. While the EPA has policies, procedures, and strategies for these function areas and domains, improvements are still needed in the following areas: • Risk Management – The EPA has not completed its corrective actions to: o Implement an enterprise Software Asset and Configuration Management capability to align license-entitlement data with software inventories. o Establish a control to validate that plans of action and milestones are created for weaknesses identified from vulnerability testing. • Configuration Management – The EPA has not updated information security procedure documentation to reflect the security-control requirements of NIST SP 800-53, Revision 4, issued on January 22, 2015. • Identity and Access Management – The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program. In addition, we found that the EPA lacks implemented processes for monitoring privileged user activity and for authorizing external access to the sampled system evaluated for this domain.



Function 0: Overall

0.2 Please provide an overall assessment of the agency's information security program. The narrative should include a description of the assessment scope, a summary on why the information security program was deemed effective/ineffective and any recommendations on next steps. Please note that OMB will include this information in the publicly available Annual FISMA Report to Congress to provide additional context for the Inspector General's effectiveness rating of the agency's information security program. OMB may modify the response to conform with the grammatical and narrative structure of the Annual Report.

·Do not include the names of specific independent auditors, these entities should be referred to as "independent assessor" or "independent auditor"

·The assessment of effectiveness should not include a list of ratings by NIST CSF Function-level, as these will already be included in the performance summary

The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The Office of the Inspector General assessed the five cybersecurity framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2020 IG FISMA reporting metrics.

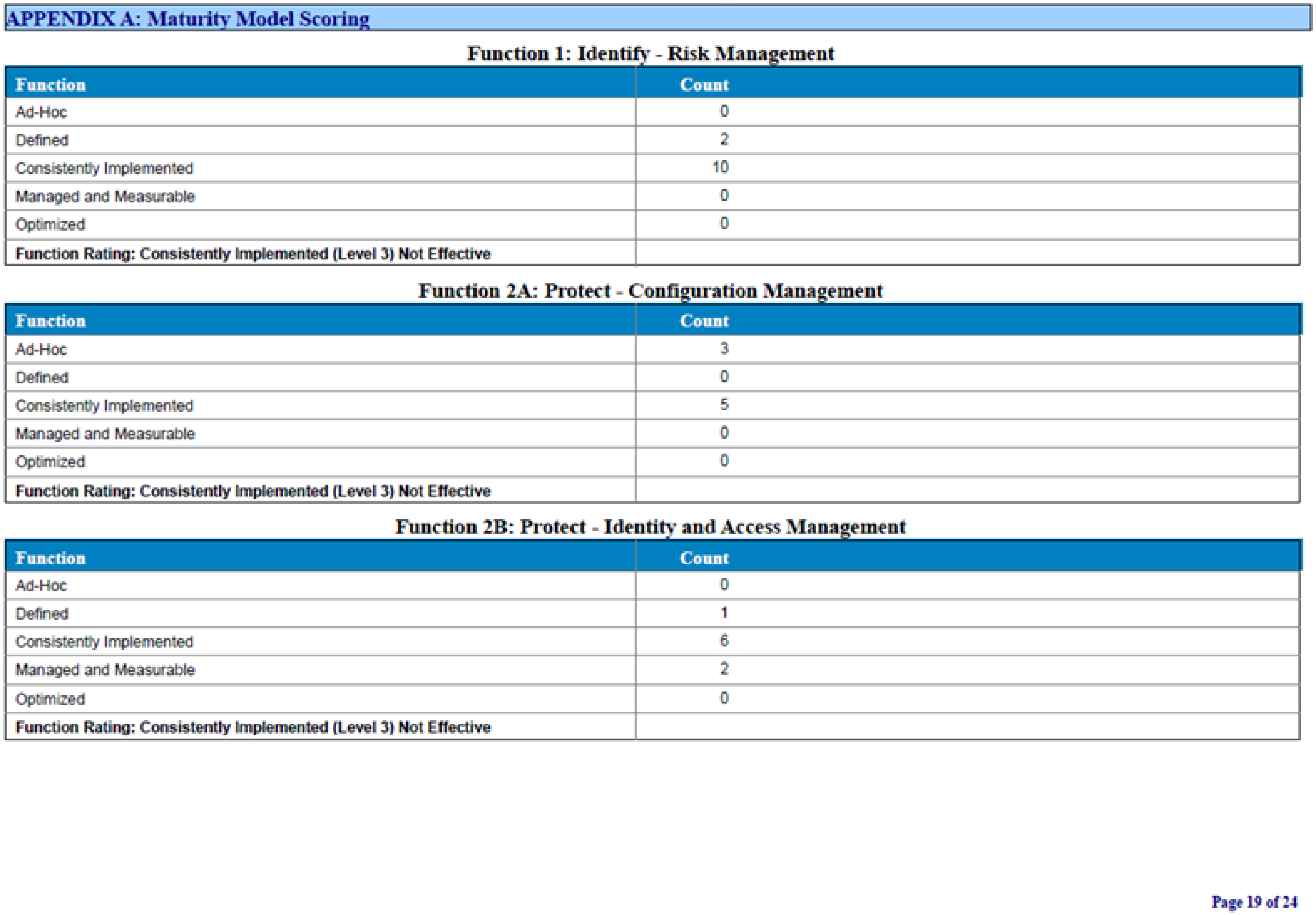
While the EPA has policies, procedures, and strategies for these function areas and domains, improvements are still needed in the following areas:

- **Risk Management – The EPA has not completed its corrective actions to:**

o Implement an enterprise Software Asset and Configuration Management capability to align license-entitlement data with software inventories.

o Establish a control to validate that plans of action and milestones are created for weaknesses identified from vulnerability testing.

- **Configuration Management – The EPA has not updated information security procedure documentation to reflect the security-control requirements of NIST SP 800-53, Revision 4, issued on January 22, 2015.**
- **Identity and Access Management – The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program. In addition, we found that the EPA lacks implemented processes for monitoring privileged user activity and for authorizing external access to the sampled system evaluated for this domain.**



APPENDIX A: Maturity Model Scoring

Function 1: Identify - Risk Management

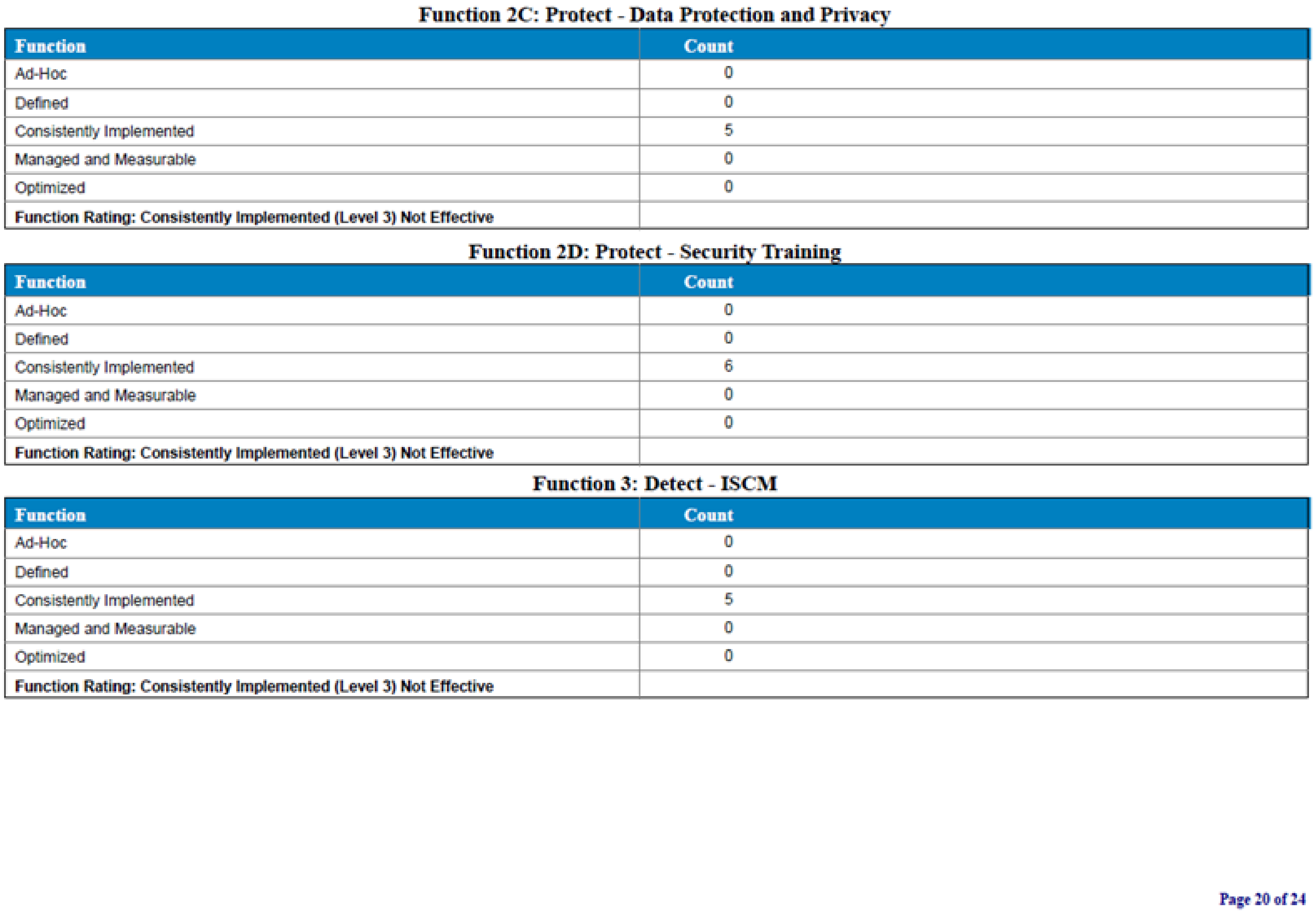
Function	Count
Ad-Hoc	0
Defined	2
Consistently Implemented	10
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2A: Protect - Configuration Management

Function	Count
Ad-Hoc	3
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2B: Protect - Identity and Access Management

Function	Count
Ad-Hoc	0
Defined	1
Consistently Implemented	6
Managed and Measurable	2
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	



Function 2C: Protect - Data Protection and Privacy

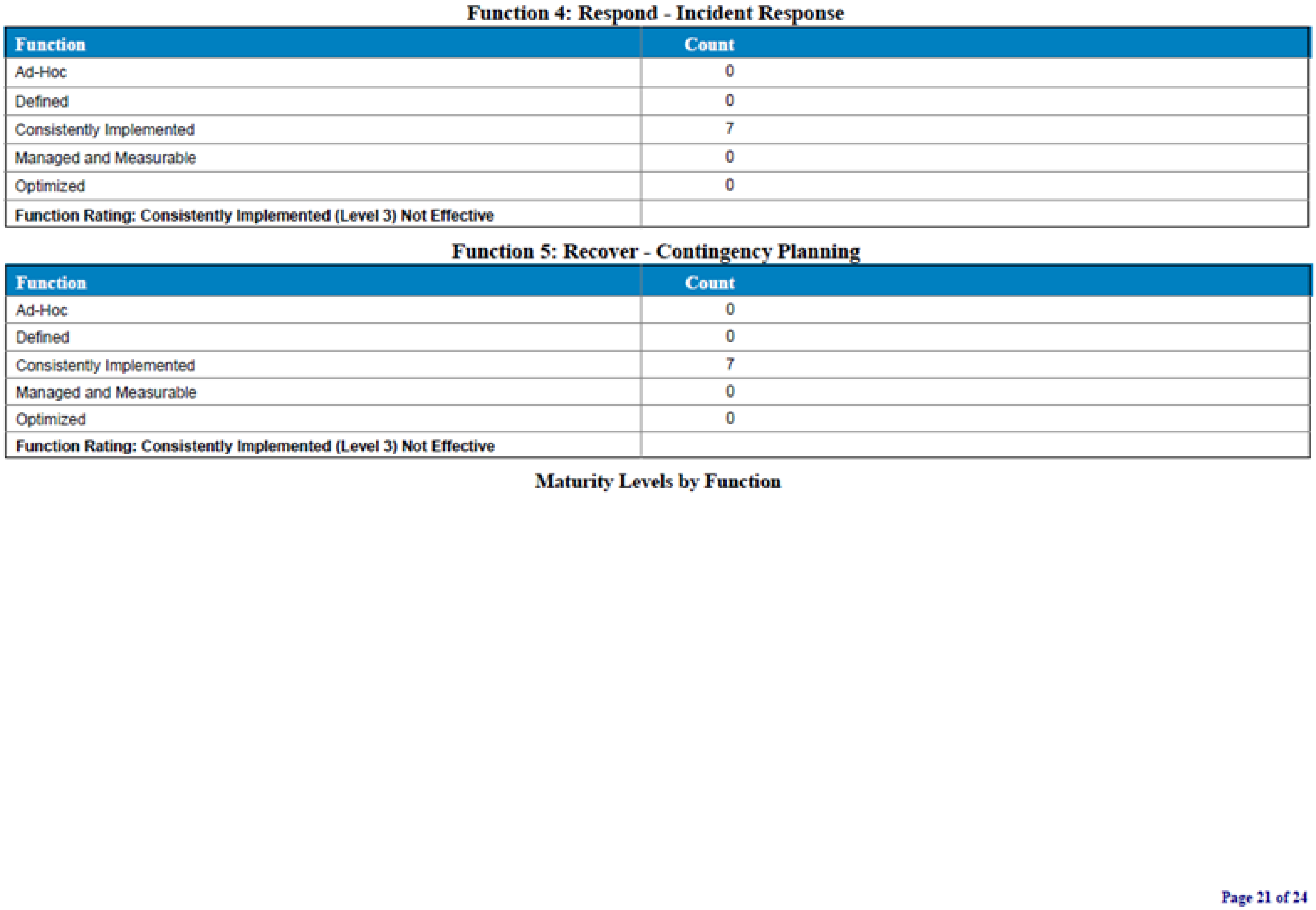
Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 2D: Protect - Security Training

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	6
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 3: Detect - ISCM

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	5
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	



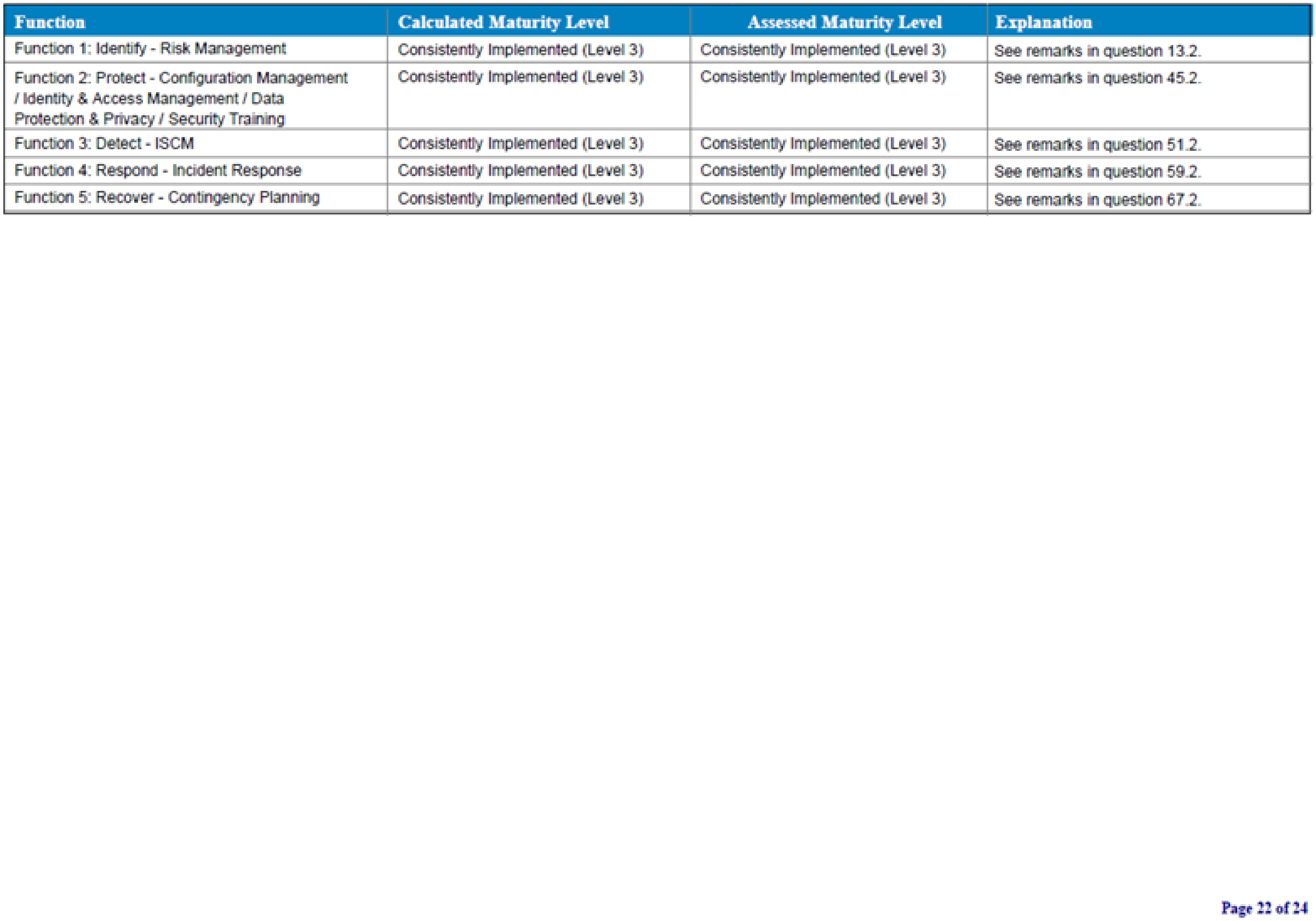
Function 4: Respond - Incident Response

Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Function 5: Recover - Contingency Planning

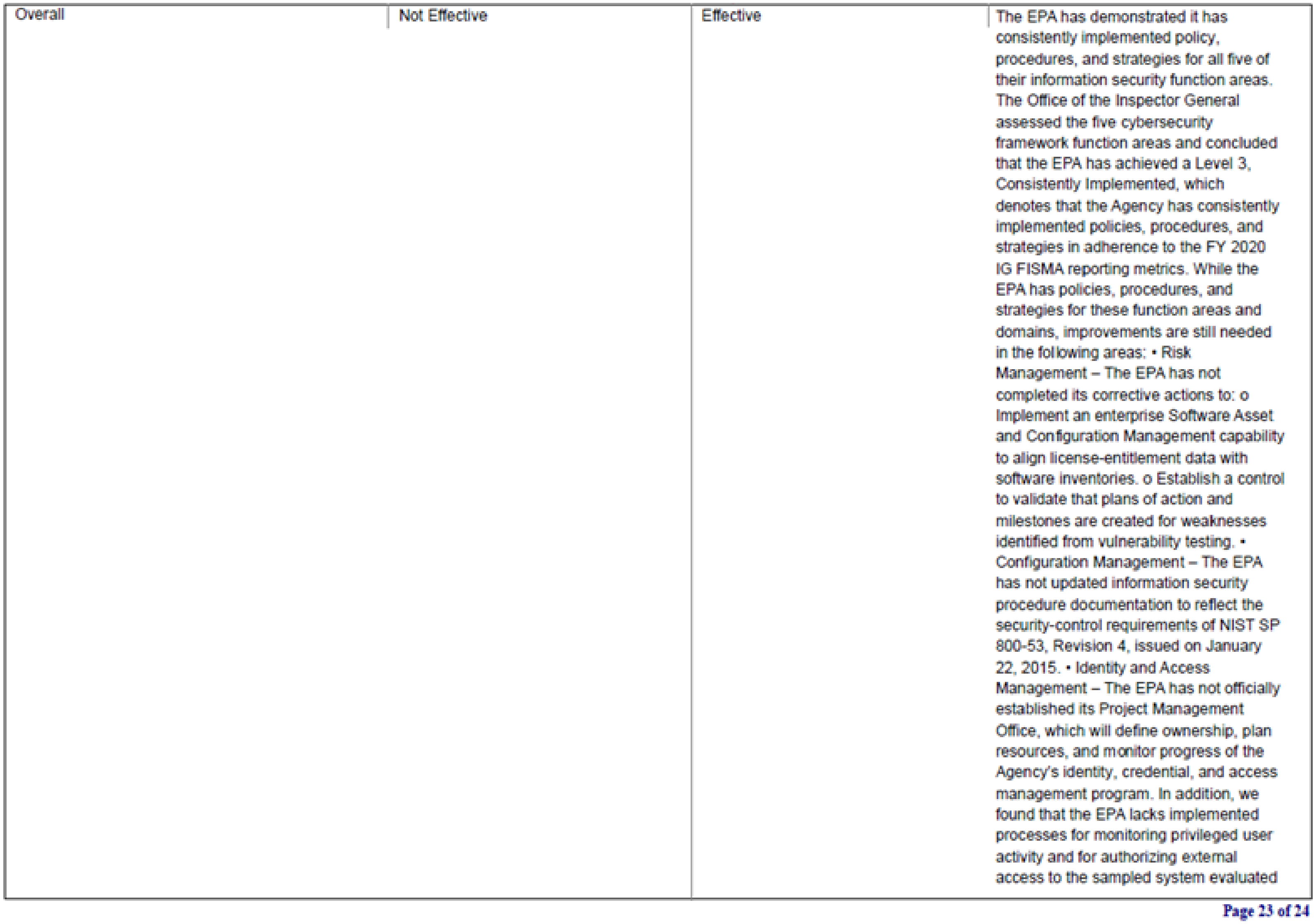
Function	Count
Ad-Hoc	0
Defined	0
Consistently Implemented	7
Managed and Measurable	0
Optimized	0
Function Rating: Consistently Implemented (Level 3) Not Effective	

Maturity Levels by Function



Function	Calculated Maturity Level	Assessed Maturity Level	Explanation
Function 1: Identify - Risk Management	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 13.2.
Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 45.2.
Function 3: Detect - ISCM	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 51.2.
Function 4: Respond - Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 59.2.
Function 5: Recover - Contingency Planning	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	See remarks in question 67.2.

Page 22 of 24



Overall	Not Effective	Effective	The EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of their information security function areas. The Office of the Inspector General assessed the five cybersecurity framework function areas and concluded that the EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the FY 2020 IG FISMA reporting metrics. While the EPA has policies, procedures, and strategies for these function areas and domains, improvements are still needed in the following areas: • Risk Management – The EPA has not completed its corrective actions to: o Implement an enterprise Software Asset and Configuration Management capability to align license-entitlement data with software inventories. o Establish a control to validate that plans of action and milestones are created for weaknesses identified from vulnerability testing. • Configuration Management – The EPA has not updated information security procedure documentation to reflect the security-control requirements of NIST SP 800-53, Revision 4, issued on January 22, 2015. • Identity and Access Management – The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency's identity, credential, and access management program. In addition, we found that the EPA lacks implemented processes for monitoring privileged user activity and for authorizing external access to the sampled system evaluated

			for this domain.

Information Security Reports Issued in FY 2020

The EPA OIG issued the following reports in FY 2020, which included recommendations regarding improvements within the EPA's information security program:

- **Report No. 20-P-0007**, *Management Alert: EPA Still Unable to Validate that Contractors Received Role-Based Training for Information Security Protection* (issued October 21, 2019). The report concluded that the EPA continues to lack information to monitor compliance with the following role-based training requirements: confirming that contractor personnel completed the required role-based training, including role-based training provisions in existing IT services contracts, and maintaining a list of contractor personnel required to complete role-based training. As a result, only seven of 21 (33 percent) EPA offices submitted a complete response by September 30, 2018, to the EPA's chief information security officer certifying that contractors completed the required role-based training. We issued this management alert on these weaknesses because immediate improvements are needed to verify that contractors are trained in their roles to protect Agency systems and data. The Agency agreed with the recommendations and completed corrective actions for Recommendations 1, 2, and 4. Recommendation 3 is considered resolved with corrective actions pending.

- **Report No. 20-P-0015**, *EPA Budget Systems Need Improved Oversight of Security Controls Testing* (issued November 1, 2019). The report concluded that the Office of the Chief Financial Officer identified the required security controls needed for the Agency's budget systems. For the Budget Automation System, the Office of the Chief Financial Officer and its service providers tested 100 percent of the security controls in our FY 2016 sample. However, they did not test all of the security controls in our FY 2017 sample. For the Budget Formulation System, the Office of the Chief Financial Officer required the cloud service provider to comply with NIST testing requirements but it did not maintain documentation to substantiate whether (1) the Budget Formulation System cloud service provider tested and implemented the required security controls or (2) the controls were working as intended to protect the Budget Formulation System and its data. Additionally, we found that the office did not correctly assign and document responsibility for testing Budget Automation System security controls and did not review the system's security reports in a timely manner or document the results of these reviews. Testing security controls enables organizations to identify vulnerabilities in their systems. Finding these vulnerabilities in a timely manner would allow the EPA to promptly remediate any weaknesses that impact the safety of its systems. Likewise, a lack of internal controls means vulnerabilities are found late or not at all and prevents the EPA from protecting its budget data from unauthorized disclosures or modifications. The Agency agreed with the recommendations and completed corrective actions for Recommendations 1 and 2.

- **Report No. 20-E-0295**, *Management Alert: EPA Region 5 Needs to Implement Effective Internal Controls to Strengthen Its Records Management Program* (issued August 31, 2020). The report concluded that Region 5 does not know whether electronic files that contained records or information subject to litigation holds were included in the files lost when the complainant migrated those files to the Agency's cloud file storage system. Additionally, Region 5 did not communicate the suspected loss of records to the agency records officer until February 2020, 11 months after the complainant learned that the files could not be recovered. As a result, Region 5 cannot verify that personnel are preserving all electronic files needed to fulfill the Agency's federal record-keeping responsibilities. Region 5 also cannot verify that an actual or suspected loss of records was communicated to the agency records officer, who would then report any loss to the National Archives and Records Administration in accordance with federal law and regulations. The Agency agreed with the recommendations and completed corrective actions for Recommendations 3, 4, and 6. Recommendations 1, 2, and 5 are considered resolved with corrective actions pending.

- **Report No. 20-E-0309**, *EPA Needs to Improve Processes for Securing Region 8's Local Area Network* (issued September 10, 2020). The report concluded that vulnerability tests of Region 8's local area network, conducted by the OMS, were not comprehensive. Additionally, wireless networks operating within the Region 8 laboratory could jeopardize controls protecting vulnerable laboratory equipment. If vulnerabilities at Region 8 are exploited, there could be denial-of-service attacks, unauthorized disclosure of personally identifiable information, and corruption of scientific data that are used to make program decisions. The Agency agreed with the recommendations and completed corrective actions for Recommendations 1, 2, 5, 6 and 7. Recommendations 3 and 4 are considered resolved with corrective actions pending.

EPA FY 2020 FISMA Compliance Results

Table C-1: Maturity level of EPA's information security function areas and domains

Security function	Security domain	OIG assessed maturity level
Identify	Risk Management	Level 3: Consistently Implemented
Protect	Configuration Management	Level 3: Consistently Implemented
Protect	Identity and Access Management	Level 3: Consistently Implemented
Protect	Data Protection and Privacy	Level 3: Consistently Implemented
Protect	Security Training	Level 3: Consistently Implemented
Detect	Information Security Continuous Monitoring	Level 3: Consistently Implemented
Respond	Incident Response	Level 3: Consistently Implemented
Recover	Contingency Planning	Level 3: Consistently Implemented
EPA's overall maturity rating: Level 3 (Consistently Implemented)		

Source: OIG test results. (EPA OIG table)

Table C-2: EPA FISMA metrics that need improvement

Security function	Security domain	Explanation of metrics areas that need improvement
Identify	Risk Management	The EPA has not implemented standard data elements to develop and maintain an up-to-date inventory of the software and associated licenses used within the organization with the detailed information necessary for tracking and reporting **(Appendix A, metric question 3)**. The EPA's plans of action and milestones were not consistently utilized for effectively mitigating security weaknesses **(Appendix A, metric question 8)**.

Protect	**Configuration Management**	The EPA has not updated information security procedures to facilitate implementation of the most recent federal security control requirements **(Appendix A, metric questions 18, 20, and 21)**.
Protect	**Identity and Access Management**	The EPA has not established a governance structure to support the Agency's ICAM program efforts **(Appendix A, metric questions 23, 24, 25).**
Protect	**Identity and Access Management**	The EPA does not monitor privileged user activity for the sampled Oracle Unified Directory system as required by federal guidance **(Appendix A, metric questions 23, 24, 25)**.
Protect	**Identity and Access Management**	The EPA has not updated information security procedures to facilitate implementation of the most recent federal security control requirements **(Appendix A, metric question 26)**.

Source: OIG test results. (EPA OIG table)

Appendix D

Agency Response to Draft Report

UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

March 23, 2021

OFFICE OF MISSION SUPPORT

MEMORANDUM

SUBJECT: Response to Office of Inspector General Draft Report Project No. OA&E-FY20-0033 "*EPA Needs to Improve Processes for Updating Guidance, Monitoring Corrective Actions, and Managing Remote Access for External Users*," dated February 24, 2021

FROM: Vaughn Noga, Chief Information Officer
Deputy Assistant Administrator for Environmental Information

VAUGHN NOGA
Digitally signed by VAUGHN NOGA
Date: 2021.03.25 07:51:14 -04'00'

TO: **Jeremy Sigel,** Team Lead
Information Resources Management Directorate
Office of Audit
Office of Inspector General

Thank you for the opportunity to respond to the subject audit report. The following summarizes the agency's overall position, along with its position on each of the report recommendations. We have provided high-level intended corrective actions for each recommendation with completion dates.

AGENCY'S OVERALL POSITION

We agree with the report's findings and have begun to develop programmatic changes which will address the concerns of the Office of Inspector General.

OMS RESPONSE TO REPORT RECOMMENDATION

No.	Recommendation	High-level Intended Corrective Action(s)	OMS Office	Estimated Completion Date
1	Update information security procedures to make them consistent with current federal directives, including the National Institute of Standards and Technology Special Publication 800-53 Revision 5, *Security and Privacy Controls*	EPA agrees with this finding and notes the majority of the IT Security policies and procedures are consistent with current federal directives. All current security assessments, implementations, and actions are completed in accordance with NIST SP 800-53r4. EPA, like other federal agencies are allowed	OISP	June 30, 2022

	for Information Systems and Organizations.	one year from the release of NIST Special Publications to update internal policies and procedures. The EPA has created a detailed project schedule to transition its current policies and procedures to NIST 800-53 Rev 5. This detail schedule includes Enterprise collaboration and inputs across all Information Security stakeholders.		
2	Establish a process where the agency follow-up official verifies that corrective actions were completed before the action official certifies that the audit report should be closed in the EPA audit tracking system.	OMS established an internal process where its audit follow-up coordinators verify that corrective actions have been completed before the action official certifies that the audit report should be closed in the EPA audit tracking system. The new template used to track corrective actions is attached. (attachment 1)	ORBO	Completed
3	Implement procedures for approving and maintaining external users' authorizations to access the web application directory system.	3.1 OMS will integrate with Login.gov (https://login.gov/) to provide external user identity vetting and authentication services for the Agency. Login.gov is a government-wide shared solution that offers the public secure and private online access to participating government programs. With a Login.gov account, external users will have their identities verified in accordance with NIST SP 800-63-3 Identity Assurance Level 1 (IAL1), self-asserted identities, and/or IAL2, remote or physically present identity proofing, before being granted access to the EPA Web Application System. 3.2 OMS will develop a periodic external user recertification process for Application Owners to follow to ensure access and authorization is limited to only users with a current need. An initial external user recertification process will take place during user migration to Login.gov as re-registration will be	OITO	December 31, 2021 December 31, 2021

		required for the existing user community.		
4	Implement procedures to monitor web application directory system privileged users' activities for unusual or suspicious activity.	OMS will coordinate with EPA System Owners, and Information Security Officers to implement processes to monitor privileged users' activities for unusual or suspicious activity. Specifically, OMS will: 4.1 Configure web applications to send all privileged user action log entries to Splunk. 4.2 Configure Splunk to identify and alert on potential suspicious privileged user activity. 4.3 Investigate all alerts and confirm incidents will be handled in accordance with EPA's Incident Response Plan.	OISP	October 15, 2021
5	Designate an integrated agencywide identity, credential, and access management office, team, or other governance structure as required by Office of Management and Budget Memorandum M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*.	The agency has designated the Chief Information Officer - Senior Advisory Council (CIO-SAC) as the governing structure for its Identity Credential and Access Management (ICAM) efforts in compliance with M-19-17. This was completed Nov 2, 2020, as part of the agency's Integrated Data Call submission to OMB. To view, see the link publicly-posted ICAM details then scroll to the bottom to see the CIO SAC listed under the heading for ICAM.	ODSTA	Completed

If you have any questions regarding this response, please contact Mitch Hauser, Audit Follow-up Coordinator, of the Office of Resources and Business Operations, (202) 564–7636 or hauser.mitchell@epa.gov.

Appendix E

Distribution

The Administrator
Assistant Deputy Administrator
Associate Deputy Administrator
Chief of Staff, Office of the Administrator
Deputy Chief of Staff, Office of the Administrator
Assistant Administrator for Mission Support
Agency Follow-Up Official (the CFO)
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for Public Affairs
Principal Deputy Assistant Administrator for Mission Support
Associate Deputy Assistant Administrator for Mission Support
Deputy Assistant Administrator for Environmental Information and Chief Information Officer, Office of Mission Support
Director, Information Security and Management Staff, Office of Mission Support
Director, IT Systems Security Staff, Office of Mission Support
Director, Office of Continuous Improvement, Office of the Chief Financial Officer
Director and Chief Information Security Officer, Office of Information Security and Privacy, Office of Mission Support
Director, Office of Information Technology Operations, Office of Mission Support
Director, Office of Resources and Business Operations, Office of Mission Support
Director, Office of Digital Services and Technical Architecture, Office of Mission Support
Audit Follow-Up Coordinator, Office of the Administrator
Audit Follow-Up Coordinator, Office of Mission Support