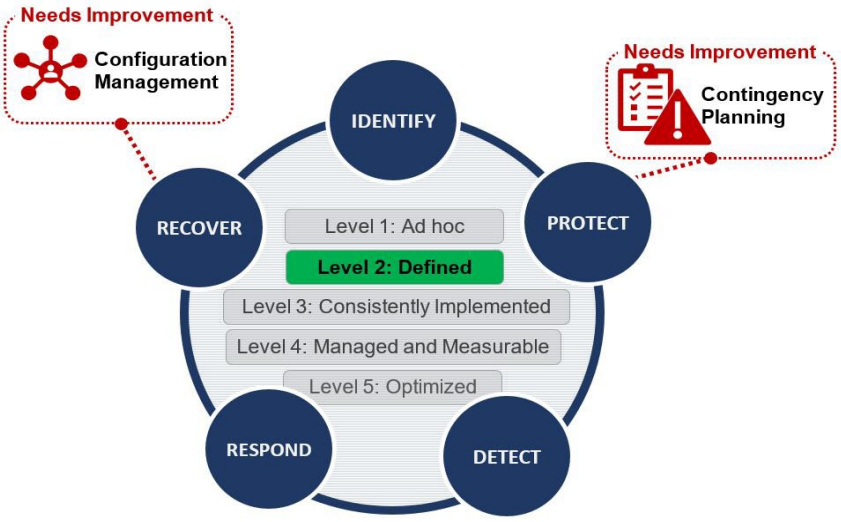
OFFICE OF INSPECTOR GENERAL
U.S. ENVIRONMENTAL PROTECTION AGENCY

CUSTOMER SERVICE ★ INTEGRITY ★ ACCOUNTABILITY

*U.S. Chemical Safety Board*

# Contractor-Produced Report: CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation

**Report No. 22-E-0025** **March 29, 2022**



| | | |
|---|---|---|
| **Abbreviations:** | CSB | U.S. Chemical Safety and Hazard Investigation Board |
| | EPA | U.S. Environmental Protection Agency |
| | FISMA | Federal Information Security Modernization Act |
| | FY | Fiscal Year |
| | IG | Inspector General |
| | OIG | Office of Inspector General |

**Cover Image:** The CSB's information security program is not consistently implemented. Improvements are needed in configuration management and contingency planning. (EPA OIG image)


**Are you aware of fraud, waste, or abuse in a CSB 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.

Office of Inspector General
U.S. Environmental Protection Agency
# At a Glance

22-E-0025
March 29, 2022

## Contractor-Produced Report: CSB Is at Increased Risk of Losing Significant Data and Is Vulnerable to Exploitation

### Why This Evaluation Was Done

This evaluation was performed to assess the U.S. Chemical Safety and Hazard Investigation Board's compliance with performance measures outlined in the fiscal year 2021 inspector general reporting instructions for the Federal Information Security Modernization Act of 2014.

SB & Company was contracted to perform this evaluation under the direction and oversight of the U.S. Environmental Protection Agency's Office of Inspector General.

The performance measures outline and provide potential ratings for security function areas to help federal agencies manage cybersecurity risks.

**This evaluation supports the CSB mission-related effort:**

- *Preventing recurrence of significant chemical incidents through independent investigations.*

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

**List of OIG reports.**

### What SB & Company Found

SB & Company assessed the effectiveness of the CSB's information security program at "Level 2, Defined," which means that the CSB's policies, procedures, and strategies for its information security program are formalized and that its strategies are documented but not consistently implemented.

**SB & Company found that the lack of off-site data backups increases the CSB's risk of losing significant data.**

While the CSB has policies, procedures, and strategies in place for the information security program, SB & Company identified that the CSB lacks a Vulnerability Disclosure Policy to protect its public website. This increases the risk that vulnerabilities identified by external stakeholders are not being reported in a timely manner to CSB management. A delay in reporting identified vulnerabilities may increase the risk of exploitation of those vulnerabilities and lead to the disruption of operations.

SB & Company also identified that the CSB discontinued the off-site storage of tape backups, which increases the risk of losing data and disrupting operations. This issue was previously identified in OIG Report No. 21-E-0071, *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, issued February 9, 2021. The CSB concurred with the recommendation in that report, implemented a corrective action, and restarted off-site backups. The CSB provided supporting documents for the corrective action taken, and we considered the corrective action for that recommendation completed. However, with the lack of on-site staff during the coronavirus pandemic, the CSB once again did not store backup tapes off-site. As a result, if the CSB headquarters loses data during an incident, those data could be permanently lost and impact the CSB's ability to fulfill its mission.

### Recommendations and Planned Agency Corrective Actions

SB & Company made two recommendations to the CSB, and the OIG agrees with and adopts these recommendations. The CSB agreed with the recommendations and provided acceptable corrective actions. The OIG considers Recommendation 1 to be resolved with corrective action completed, and Recommendation 2 to be resolved with corrective action pending.

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

THE INSPECTOR GENERAL

March 29, 2022

Katherine A. Lemos, Ph.D.
Chairperson and Chief Executive Officer
U.S. Chemical Safety and Hazard Investigation Board
1750 Pennsylvania Avenue NW, Suite 910
Washington, D.C. 20006

Dear Dr. Lemos:

This is a report on the U.S. Chemical Safety and Hazard Investigation Board's information security program. The report synopsizes the results of information technology security work performed by SB & Company under the direction of the U.S. Environmental Protection Agency's Office of Inspector General. This report also includes SB & Company's completed fiscal year 2021 Federal Information Security Management Act reporting template, as prescribed by the Office of Management and Budget. The project number for this evaluation is OA-FY21-0205. This evaluation was conducted in accordance with *Quality Standards for Inspection and Evaluation*, published in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

This report contains SB & Company's findings and recommendations. We agree with SB & Company's recommendations and adopt them as our own.

Your staff provided acceptable corrective actions in response to the recommendations. All recommendations are resolved, and no final response to this report is required. If you submit a response, however, 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.

Sincerely,

Sean W. O'Donnell

Sean W. O'Donnell

# *Table of Contents*

**SB & Company Report ..... 1**

**CSB Response and OIG Assessment ..... 7**

**Status of Recommendations ..... 8**

## Appendixes

B Status of CSB Corrective Actions for FY 2018, FY 2019, and FY 2020 FISMA Report Recommendations ..... 38
C CSB Response to Report ..... 40
D Distribution ..... 41

## Report of Independent Public Accountants

To the Management of *U.S. Chemical Safety and Hazard Investigation Board*:

This report presents the results of our independent evaluation of the U.S. Chemical Safety and Hazard Investigation Board (CSB)'s information security program and practices. The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies, including CSB, to have an annual independent evaluation performed of their information security program and practices and to report the results of the evaluations to the Office of Management and Budget (OMB). OMB has delegated its responsibility for the collection of annual FISMA responses to the Department of Homeland Security (DHS). DHS, in conjunction with OMB and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), developed the Fiscal Year (FY) 2021 FISMA Reporting Metrics to collect these responses. FISMA requires the agency Inspector General (IG) or an independent external auditor to perform the independent evaluation as determined by the IG. The Environmental Protection Agency Office of Inspector General (OIG) contracted SB & Company, LLC (SBC) to conduct this independent evaluation and monitored our work to ensure we met professional standards and contractual requirements.

We conducted our independent evaluation in accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

The objective for this independent evaluation was to assess the effectiveness of CSB's information security program and practices, including CSB's compliance with FISMA and related information security policies, procedures, standards, and guidelines for the period October 1, 2020, to September 30, 2021. We based our work on a selection of CSB-wide security controls and a selection of system specific security controls across CSB information systems. Additional details regarding the scope of our independent evaluation are included in the report, Background, Scope, and Methodology. Appendix A contains the FISMA Matrix and Appendix B the status of prior year recommendations.

Consistent with applicable FISMA requirements, OMB policy and guidance, and National Institute of Standards and Technology (NIST) standards and guidelines, CSB established and maintained its information security program and practices for its information systems for the five cybersecurity functions and eight FISMA metric domains. Based on the results entered into CyberScope, we determined that CSB's overall information security program was "Defined" because a majority of the FY 2021 FISMA metrics were rated Defined (Level 2). We reported deficiencies impacting specific CyberScope questions in Identify (supply chain risk management) and Protect (configuration management).

In our report, we have provided the Chief Information Officer (CIO) two findings and two recommendations that when addressed should strengthen CSB's information security program. The CSB CIO agreed with our conclusions and recommendations (see Management Response, page 44).

This independent evaluation did not constitute an engagement in accordance with Generally Accepted Government Auditing Standards. SB & Company, LLC did not render an opinion on CSB's internal controls over financial reporting or over financial management systems as part of this evaluation. We caution that projecting the results of our evaluation to future periods or other CSB information systems not included in our selection is subject to the risk that controls may become inadequate because of changes in technology or because compliance with controls may deteriorate.

Washington, D.C.
January 14, 2022

# *Table of Contents*


**Background** ---------- 1

**Scope and Methodology** ---------- 2

**Prior Audit** ---------- 4

**Results** ---------- 5

**Conclusion** ---------- 6

**Recommendations** ---------- 6


## Appendix

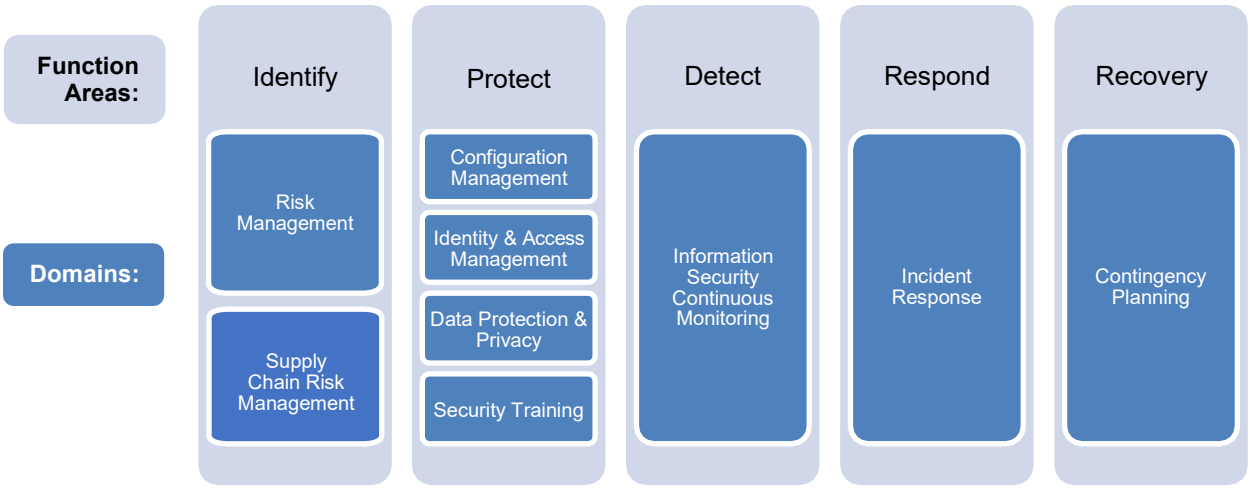

**A SB & Company-Completed Department of Homeland Security CyberScope Template** ---------- 9

## Background

Under the Federal Information Security Modernization Act of 2014 (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.

Each fiscal year, the U.S. Department of Homeland Security and the Office of Management and Budget issue an *IG FISMA Reporting Metrics* template for the Inspector General of each federal agency to use to assess the agency's information security program. The *FY 2021 IG FISMA Reporting Metrics*,[1] which can be found in Appendix A, identifies nine domains within the five security functions defined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity (Figure 1).[2] This cybersecurity framework provides agencies with a common structure for identifying and managing cybersecurity risks to critical infrastructure across the enterprise.

**Figure 1: FY 2021 cybersecurity framework security function areas and domains**




Source: OIG-created graphic based on *FY 2021 IG FISMA Reporting Metrics* information.

The effectiveness of an agency's information security program is based on a five-tiered maturity model spectrum (Table 1). An agency's IG is 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 nine domains. The IG makes this determination by answering a series of questions

[1] *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics,* Version 1.1, dated May 12, 2021. These metrics were developed as a collaborative effort between the Office of Management and Budget, the Department of Homeland Security, and the Council of the Inspectors General on Integrity Management and Efficiency, in consultation with the Federal Chief Information Officer Council

[2] Executive Order 13636, Improving Critical Infrastructure Cybersecurity, was issued February 19, 2013, and directed NIST to develop a voluntary framework based on existing standards, guidelines, and practices to reduce cyber risks to critical infrastructure.

about the domain-specific criteria that are presented in the annual *IG FISMA Reporting Metrics* template.

An agency must fully satisfy each maturity level before it can be evaluated at the next maturity level. This approach requires the agency to develop the necessary policies, procedures and strategies during the foundational levels (1 and 2). The advanced levels (3, 4 and 5) describe the extent to which the agencies have institutionalized those policies and procedures.

**Table 1: Maturity model spectrum**

| Maturity level | | Description |
|---|---|---|
| 1 | Ad Hoc | Policies, procedures and strategies are not formalized; activities are performed in an ad hoc, reactive manner. |
| 2 | Defined | Policies, procedures and strategies are formalized and documented but not consistently implemented. |
| 3 | Consistently Implemented | Policies, procedures and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking. |
| 4 | Managed and Measurable | 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. |
| 5 | Optimized | Policies, procedures and strategies are fully institutionalized, repeatable, self-generating, consistently implemented and regularly updated based on a changing threat and technology landscape and business/mission needs. |

Source: *FY 2021 IG FISMA Reporting Metrics*.

## Scope and Methodology

SB & Company, LLC (SBC or We) conducted this evaluation from June to October 2021 in accordance with accordance with CIGIE Quality Standards for Inspection and Evaluation and applicable American Institute of Certified Public Accountants (AICPA) standards.

During our evaluation, we assessed whether the CSB exceeded Maturity Level 1, *Ad-Hoc*, for each of the 66 questions for the nine domains in the *FY 2021 IG FISMA Reporting Metrics*. We conducted a risk assessment of the FY 2021 IG FISMA metrics to determine whether changes made to the underlying criteria of the FISMA metric questions significantly changed since the FY 2020 evaluation.

We also evaluated the new FY 2021 criteria to assess whether they significantly changed the CSB's responses to the overall metric questions since the FY 2020 evaluation. We assessed each new criterion as either:

- High Risk—The Office of Management and Budget introduced new reporting metrics, or the CSB made significant changes to its information security program since the FY 2020 evaluation for the identified metric question.

- Low Risk—The CSB made no significant changes to its information security program since the FY 2020 evaluation for the identified metric question.

We relied on the responses to the FY 2020 CSB FISMA metric questions to answer the FY 2021 metric questions rated as *low risk*, and we conducted additional evaluation work to answer the questions rated as *high risk*.

We limited our assessment to determine whether the agency possessed the noted policies, procedures and strategies required for each metric under the function area. If the policies, procedures and strategies were formalized and documented, we rated the agency at Level 2, Defined. If not, we rated the agency at Level 1, *Ad Hoc*.

We worked with the CSB and briefed the agency on the evaluation results for each function area of the *FY 2021 IG FISMA Reporting Metrics*.

Appendix A provides the OIG response to each FISMA metric, as submitted to the Office of Management and Budget on October 31, 2021.

## *Prior Audit*

During our testing of the CSB's FY 2021 FISMA compliance, SBC followed up on deficiencies identified in the FY 2020 FISMA evaluation, as documented in Report No. 21-E-0071 CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses, dated February 9, 2021. We reported that the CSB lacked documented procedures and needed improvement in one domain: (1) Identity and Access Management. Specifically, SBC found that the CSB did not:

1. Complete the Risk Assessment process as required by NIST 800-37 re-evaluate the Risk Management Framework to make in more fluent to leverage day-to-day processes in place for completing the risk assessment and determine how to best implement an organization-wide governance process for monitoring and reporting on risks.
2. Document the process in place to monitor required flaw remediation to resolution and enhance the flaw remediation process to require approvals if risks cannot be mitigated to an acceptable level in a timely manner. In addition, develop timeframes and monitoring on the timeliness of applying patch updates.
3. Implement a process to ensure that privacy awareness training is provided to all individuals, including role-based training where needed.
4. Implement Information Security awareness and specialized security training policies and procedures to provide exposure to areas specific to individuals that have a role supporting Information Security or technology related areas. In addition, document an Information Security awareness and training strategy that leverages its organizational skills assessment and factors the training program priorities, funding, the goals of the program, and targeted audiences.
5. Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media offsite.

The CSB completed corrective actions for recommendation 3 listed above. See Appendix B for more details on the status of these corrective actions.

# Results

The CSB's information security program is assessed overall at Maturity Level 2, Defined. Table 2 specifies the maturity level for each function area and the associated domains.

**Table 2: Maturity level of reviewed CSB function areas and domains**

| Function area | Domain | Overall OIG-assessed maturity level |
|---|---|---|
| Identify | Risk Management | Level 2, *Defined* |
| Identify | Supply Chain Risk Management | Level 1, *Ad-Hoc* |
| Protect | Configuration Management | Level 2, *Defined* |
| Protect | Identity and Access Management | Level 2, *Defined* |
| Protect | Data Protection and Privacy | Level 2, *Defined* |
| Protect | Security Training | Level 2, *Defined* |
| Detect | Information Security Continuous Monitoring | Level 2, *Defined* |
| Respond | Incident Response | Level 2, *Defined* |
| Recover | Contingency Planning | Level 2, *Defined* |

Source: *FY 2021 IG FISMA Reporting Metrics*.

However, in FY 2021, the CSB continued to need improvements for a specific question in the "Configuration Management" and "Contingency Planning" domains, as shown in Table 3.

**Table 3: CSB domains that require further improvement**

| Function area | Domain | FISMA questions that need improvement |
|---|---|---|
| Protect | Configuration Management | The CSB has not published a Vulnerability Disclosure Police to their public facing website. *See Appendix A, FISMA Question 24.* |
| Recover | Contingency Planning | The CSB does not consistently store system backups offsite at a sufficient distance from its headquarters. Lack of consistent, off-site backups increases the risk of loss of data and a disruption to operations. See *Appendix A, FISMA Question 64.* |

Source: SBC analysis

## Conclusion

The CSB would improve and strengthen its cybersecurity program by publishing a Vulnerability Disclosure Policy (VDP) on its public facing websites. A VDP will provide ethical hackers instruction on how to report vulnerabilities that they have identified and promote cooperation between internal and external stakeholders pertaining to vulnerabilities.

The CSB would also improve its cybersecurity program by consistently storing system backups at an offsite location a sufficient distance from its headquarters. Due to lack of on-site staffing during the COVID-19 pandemic, the offsite storage of tape backups was discontinued. Lack of consistent, off-site backups increases the risk of loss of data and a disruption to operations. In the case of an incident that causes the loss of the CSB's headquarters, this lack of off-site backups could lead to significant loss of data and impact the agency's ability to fulfill its mission.

## Recommendations

We recommend that the Chairperson for the U.S. Chemical Safety and Hazard Investigation Board:

1. Develop and deploy a Vulnerability Disclosure Policy to formalize security feedback and to comply with Office and Management and Budget M-20-32 and U.S. Department of Homeland Security Binding Operational Directive 20-01.

2. Immediately restore off-site storage of backup tapes and implement a strategy that will ensure that the Agency consistently stores backups of its systems at an off-site location. Additionally, explore alternative methods of off-site backup that can be performed automatically and do not require physical intervention by CSB personnel, such as storing backups in the cloud.

## *CSB Response and OIG Assessment*

The CSB agreed with the recommendations and provided acceptable corrective actions. With respect to Recommendation 1, the CSB stated it approved and published a Vulnerability Disclosure Policy to the CSB website in accordance with the recommendation. The OIG reviewed the CSB website and verified that the Vulnerability Disclosure Policy was posted. The OIG considers this recommendation resolved with corrective action completed.

With respect to Recommendation 2, the CSB stated that it has resumed off-site manual backup procedures, hired a new agency purchasing officer, and conducted preliminary market research to understand its need for cloud services. The OIG considers this recommendation resolved with corrective action pending.

# *Status of Recommendations*

**RECOMMENDATIONS**

| Rec. No. | Page No. | Subject | Status[1] | Action Official | Planned Completion Date |
|---|---|---|---|---|---|
| 1 | 6 | Develop and deploy a Vulnerability Disclosure Policy to formalize security feedback and to comply with Office and Management and Budget M-20-32 and U.S. Department of Homeland Security Binding Operational Directive 20-01. | C | Chairperson | 3/15/22 |
| 2 | 6 | Immediately restore off-site storage of backup tapes and implement a strategy that will ensure that the Agency consistently stores backups of its systems at an off-site location. Additionally, explore alternative methods of off-site backup that can be performed automatically and do not require physical intervention by CSB personnel, such as storing backups in the cloud. | R | Chairperson | 7/15/22 |

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

**Appendix A**

# *SB & Company-Completed Department of Homeland Security CyberScope Template*

This section shows the information uploaded to the Department of Homeland Security's CyberScope program by the EPA OIG, based on the template completed by the SB & Company.

# Inspector General

Section Report

2021

IG Annual

## Chemical Safety Board

## Function 0: Overall

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

Effective

**Comments: The U.S. Chemical Safety and Hazard Investigation Board's Information Security Program has demonstrated that it has defined policy, procedures, and strategies for all five of its information security function areas.**

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.

The U.S. Chemical Safety and Hazard Investigation Board's Information Security Program has demonstrated that it has defined policy, procedures, and strategies for all five of its information security function areas. The Office Cybersecurity Framework function areas and concluded that CSB has achieved a Level 2, "Defined", which denotes that the Agency has defined policies, procedures and strategies in adherence to the Fiscal Year 2021 Inspector General Federal Information Security Modernization Act reporting metrics. While CSB has policies, procedures and strategies for these function areas and domains, improvements are still needed in the configuration Management area; CSB has not published its Risk Assessment or Systems and Information Integrity procedures to meet the U.S> Department of Homeland Security Binding Operational Directive 19-02, "Vulnerability Remediation Requirements for Internet-Accessible Systems", a federal requirement for remediating critical vulnerabilities within 15 calendar of initial detection.

## Function 1A: 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 2021 CIO FISMA Metrics: 1.1, 1.1.5 and 1.4, OMB A-130, NIST SP 800-37, Rev. 2: Task P-18).

Defined (Level 2)

**Comments: CSB has a defined process to maintain a comprehensive inventory of its information systems.**

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 2021 CIO FISMA Metrics: 1.2, 1.3, 2.2, 3.9, CSF: ID.AM-1; NIST SP 800-37, Rev. 2: Task P-10).
Defined (Level 2)

**Comments: CSB has a defined process to maintain a comprehensive inventory of its information systems.**

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 2021 CIO FISMA Metrics: 1.2.5, 1.3.3, 1.3.9, 1.3.10, 3.10; CSF: ID.AM-2; NIST SP 800-37, Rev. 2: Task P-10)?
Defined (Level 2)

**Comments: CSB has a defined process for using standard data elements and taxonomy to develop and maintain an up-to-date inventory of software assets and licenses used in the organization's environment with the detailed information necessary for tracking and reporting.**

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 2021 CIO FISMA Metrics: 1.1; OMB M-19-03; NIST SP 800-37, Rev. 2: Task C-2, C-3, P-12, P-13, S-1 - S-3 )?
Defined (Level 2)

**Comments: CSB has categorized and communicated the importance and priority of information systems in enabling its milestone mission and business functions, including for high-value assets.**

5. To what extent does the organization ensure that information system security risks are adequately managed at the organizational, mission/business process, and information system levels (NIST SP 800-39; NIST SP 800-53 Rev. 4: RA-3, PM-9; NISTIR 8286, CSF: ID RM-1 - ID.RM-3; OMB A-123; OMB M-16-17; Green Book (Principle #6); OMB M-17-25; NIST SP 800-37 (Rev. 2): TasksR-2, R-3, P-14?
Defined (Level 2)

**Comments: CSB has defined and communicated the policies, procedures and processes it uses to manage the cybersecurity risk associated with operating and maintaining its information systems.**

## Function 1A: Identify - Risk Management

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) Task P-16; 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)?
**Defined (Level 2)**

**Comments: CSB has defined the information security architecture and described how that architecture is integrated into and supports CSB's enterprise architecture.**

7. To what degree have roles and responsibilities of internal and external stakeholders involved in cyber security risk management processes been defined and communicated across the organization (NIST SP 800-39: Section 2.3.1, 2.3.2, and Appendix D; NIST SP 800-53 Rev. 4: RA-1; CSF: ID.AM-6, ID.RM-1, and ID.GV-2; NISTIR 8286, Section 3.1.1, OMB A-123;; NIST SP 800-37 (Rev. 2) Section 2.8 and Task P-1; OMB M-19-03)?
**Defined (Level 2)**

**Comments: The roles and responsibilities of stakeholders involved in cybersecurity risk management have been defined and communicated across CSB.**

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) Task A-6, R-3; OMB M-19-03, CSF v1.1, ID.RA-6)?
**Ad Hoc (Level 1)**

**Comments: CSB has implemented an information technology for its plan of action and milestones monitoring with defined time frames for remediating security weaknesses; however, there is not a documented procedure in place that defines how the results from the monitored tracking sheets will be used to mitigate any security weakness identified. defined the information security architecture and described how that architecture is integrated into and supports CSB's enterprise architecture.**

## Function 1A: Identify - Risk Management

9. To what extent does the organization ensure that information about cyber security risks is communicated in a timely manner to all necessary internal and external stakeholders (OMB A-123; OMB Circular A-11; Green Book (Principles #9, #14 and #15); OMB M-19-03; CSF: Section 3.3; NIST SP 800-37 (Rev. 2) Task M-5; SECURE Technology Act: s. 1326, NISTIR 8286)?
Defined (Level 2)

**Comments: CSB has defined how cybersecurity risks are communicated in a timely and effective manner to appropriate internal and external stakeholders.**

10. To what extent does the organization utilize technology/ automation to provide a centralized, enterprise wide (portfolio) view of cybersecurity risk management activities 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)?
Ad Hoc (Level 1)

**Comments: While a risk assessment process is in place, a risk assessment has not been performed in the last 12 months due to the ongoing effects of the pandemic.**

11.1. Please provide the assessed maturity level for the agency's Identify - Risk Management program.
Defined (Level 2)

**Comments: Based on the maturity level of the individual areas within Risk Management, the domain is concluded as "Defined."**

11.2. 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?
Based on the maturity level of the individual areas within Risk Management, the overall maturity level is concluded as "Defined". We limited our testing to those questions with criteria added to the metric that would materially change our Fiscal Year 2020 response. For those metrics whose; policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined". However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

## Function 1B: Identify - Supply Chain Risk Management

12. To what extent does the organization utilize wide supply chain risk management policies and procedures to manage SCRM activities at all organizational tiers (NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-1, NIST CSF v1.1, ID.SC-1, NIST 800-161)?

Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formerly document

13. To what extent does the organization utilize a supply chain risk management plan(s) to ensure the integrity, security, resilience, and quality of services, system components, and systems (OMB A-130, NIST SP 800-37 Rev. 2, Section 2.8, NIST 800-53, SR-2, SR-3; NIST 800-161, section 2.2.4 and Appendix E)?

Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formerly document

14. To what extent does the organization ensure that products, system components, systems, and services of external providers are consistent with the organization's cybersecurity and supply chain requirements. (NIST SP 800-53 REV. 5: SA-4, SR-3 - 6; NIST SP 800-152; NIST SP 800-37 Rev. 2, Section 2.8; FedRAMP standard contract clauses; Cloud Computing Contract Best Practices; OMB M-19-03; OMB A-130; CSF: ID.SC-2 through 4).

Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formerly document

15. To what extent does the organization maintain and monitor the provenance and logistical information of the systems and system components it acquires? (NIST SP 800-53 REV. 5: SR-4 and NIST SP 800-161, Provenance (PV) family)?

Ad Hoc (Level 1)

Comments: Due to the size and resources of the organization, processes related to supply chain risk management are not formerly document

## Function 1B: Identify - Supply Chain Risk Management

16.1. Please provide the assessed maturity level for the agency's Identify - Supply Chain Risk Management program.
Ad Hoc (Level 1)

Comments: Based on the maturity level of the individual areas within Supply Chain Risk Management, the domain is concluded as "Ad Hoc."

16.2. Please provide the assessed maturity level for the agency's Identify Function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, the Identify function is concluded as "Defined."

16.3. Provide any additional information on the effectiveness (positive or negative) of the organization's Supply Chain Risk Management domains, 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?
Based on the maturity level of the individuals areas within the Risk Management and Supply Chain Risk Management domains, the identity function is concluded as "Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2929 responses. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined". However, we did not test to determine what additional steps the Agency needs to complete to activate a higher maturity level.

## Function 2A: Protect - Configuration Management

17. 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)?
Defined (Level 2)

Comments: CBS has defined and communicated across the organization the roles and responsibilities at the organizational and information system levels for stakeholders involved in information system configuration management.

## Function 2A: Protect - Configuration Management

18. 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)?

**Defined (Level 2)**

Comments: CBS Configuration Management policy defines roles and responsibility for configuration management. The policy also defines processes included in change management and the system development life cycle. communicated across the organization the roles and

19. 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 2021 CIO FISMA Metrics: 2.2, 3.9.2, and 3.10.1; CSF: DE.CM-7 and PR.IP-1)?

**Defined (Level 2)**

Comments: CBS has developed, documented and disseminated its baseline configuration and component inventory policies and procedures.

20. 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 2021 CIO FISMA Metrics: 2.1, 2.2, 4.3; SANS/CIS Top 20 Security Controls 3.7; CSF: ID.RA-1 and DE.CM-8)?

**Defined (Level 2)**

Comments: CBS has developed, documented and disseminated its policies and procedures for configuration settings and common secure configurations. In addition, CSB has developed, documented and disseminated common secure configurations (hardening guides) that are tailored to its environment.

## Function 2A: Protect - Configuration Management

21. 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 2021 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 BOD18-02)?
Ad Hoc (Level 1)

Comments: CBS has implemented an Information Technology Plan of Actions and Milestone monitoring tracking sheet including patch management, with a defined time frame for remediation security weaknesses; however, there is not a documented procedure in place that defines how the monitoring tracking sheet will be used to mitigate any security weaknesses identified and the policies and procedures for flaw remediation have not been disseminated across the organization.

22. To what extent has the organization adopted the Trusted Internet Connection (TIC) program to assist in protecting its network (OMB M-19-26)?
Defined (Level 2)

Comments: CBS has adopted the Trusted Internet Connection program utilizing a Verizon Managed Trusted Internet Protocol Services monitored by the Department of Homeland Security.

23. 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).
Defined (Level 2)

Comments: CBS has developed, documented, and disseminated its policies and procedures for managing configuration change control. The policies and procedures address the review and approval and disapproval of proposed changes, retaining records of implemented changes, and coordination and oversight of changes by CSB.

## Function 2B: Protect - Identity and Access Management

24. To what degree does the organization utilize a vulnerability disclosure policy (VDP) as part of its vulnerability management program for internet-accessible federal systems (OMB M-20-32 and DHS BOD 20-01)?
Ad Hoc (Level 1)

Comments: CBS has not developed or deployed a Vulnerability Disclosure to the Agency's public-facing website.

25.1. Please provide the assessed maturity level for the agency's Protect - Configuration Management program.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Configuration Management, the domain is concluded as "Defined."

25.2. 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?

Based on the maturity level of the individual areas within Configuration Management, the domain is concluded as "Defined." We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. I f the policies, procedures and strategies were documented, we rated the CSB at Level 2, "Defined". However, we did not test to determine what additional steps the Agency needs to complete to achieve higher maturity level.

26. To what extent 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; NIST SP 800-63-3 and 800-63A, B, and C; Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance (FICAM), OMB M-19-17)?
Consistently Implemented (Level 3)

Comments: The CSB has defined, communicated, and appropriately resourced the roles and responsibilities for indent, credential, and access management.

## Function 2B: Protect - Identity and Access Management

27. To what extent does the organization utilize a comprehensive ICAM policy, strategy, process, and technology solution roadmap to guide its ICAM processes and activities (FICAM, OMB M-19-17; NIST SP 800-53 REV. 4: AC-1 and IA-1; OMB M-19-17, 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: CSB has developed, documented, and disseminated its policies and procedures for identity, Credential and Access

28. To what extent has the organization developed and implemented processes for assigning position risk designations and performing appropriate personnel 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, OMB M-19-17)?
**Defined (Level 2)**

Comments: CSB has defined its processes for ensuring that all personnel are assigned risk designation, and appropriately screened prior to being granted access to its systems.

29. 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 PS-6)?
**Defined (Level 2)**

Comments: CSB has defined its processes for developing, documenting, and maintaining access agreements for individuals that access its systems.

30. To what extent has the organization implemented strong authentication mechanisms (PIV or an Identity Assurance Level (IAL)3/Authenticator Assurance Level (AAL) 3 credential) for non-privileged users to access the organization's facilities [organization-defined entry/exit points], networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17, IA-2, IA-5, IA-8, and PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; FY 2021 CIO FISMA Metrics: 2.4, 2.7, CSF: PR.AC-1 and 6; OMB M-19-17, and NIST SP 800-157,)?
**Defined (Level 2)**

Comments: CSB has implemented strong authentication mechanisms in the use of virtual private network to remotely access the internal internet. The VPN tunnel is defined on points into the network. In addition, the user must be added to the VPN group on the Active Directory to access the CSB ne Multifactor authentication is used to secure access for individuals with escalated permissions.

## Function 2B: Protect - Identity and Access Management

31. 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 [organization-defined entry/exit points], networks, and systems, including for remote access (CSIP; HSPD-12; NIST SP 800-53 REV. 4: AC-17, PE-3; NIST SP 800-128; FIPS 201-2; NIST SP 800-63, 800-157; OMB M-19-17, FY 2021 CIO FISMA Metrics: 2.3, 2.5, and 2.7; CSF: PR.AC-1 and 6; and DHS ED 19-01)?

**Defined (Level 2)**

Comments: CSB has implemented multifactor authentication for all users including privileged users with escalated permissions.

32. 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 2021 CIO FISMA Metrics: 2.3, 2.5, 2.6, and 2.7; OMB M-19-17, NIST SP 800-53 REV. 4: AC-1, AC-2, AC-5, AC-6, AC-17; AU-2, AU-3, AU-6, and IA-4; CSIP; DHS ED 19-01; CSF: PR.AC-4).

**Defined (Level 2)**

Comments: CSB has defined its processes for provisioning, managing, and reviewing privileged accounts.

33. 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-11, AC-12, AC-17, AC-19, AU-2, IA-7, SC-10, SC-13, and SI-4; CSF: PR.AC-3; and FY 2021 CIO FISMA Metrics: 2.10 and 2.11).

**Defined (Level 2)**

Comments: CSB uses VPN Connection to provide remote access. CSB has defined its configuration and connection requirements for remote access connections, including the use of cryptographic modules, system time-outs, and the monitoring and controls of remote access sessions.

## Function 2B: Protect - Identity and Access Management

34.1. Please provide the assessed maturity level for the agency's Protect - Identity and Access Management program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Identity and Access Management, the domain is concluded as "Defined."

34.2. 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?

Based on the maturity level of the individual areas within identity and Access Management, the domain is concluded as "Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined". However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

## Function 2C: Protect - Data Protection and Privacy

35. 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) Section 2.3, Task P-1 ; OMB M-20-04; OMB M-19-03; OMB A-130, Appendix I; CSF: ID.GV-3; NIST SP 800-53 REV. 4: AR-4 and Appendix J, FY 2020 SAOP FISMA metrics, Sections 1 through 4, 5(b))?

Defined (Level 2)

Comments: CSB has defined and communicated its privacy program plan and related policies and procedures for the protection of personal identifiable information that is collected, used, maintained, shared and disposed of by its information systems. In addition, roles and responsibilities for the effective implementation of CSB's privacy program have been defined and CSB has determined the resources and optimal governance structure needed to effectively implement its privacy program.

36. 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 2021 CIO FISMA Metrics: 2.8, 2.12; 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

Defined (Level 2)

Comments: CSB's policies and procedures have been defined and communicated for the specified areas.

37. 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 2021 CIO FISMA Metrics: 3.8; DHS BOD 18-01; DHS ED 19-01; CSF: PR.DS-5)?

Defined (Level 2)

Comments: CSB has implemented security controls to prevent data exfiltration and enhance network defenses.

38. 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 2020 SAOP FISMA metrics, Section 12; OMB M-17-12; and OMB M-17-25)?

Defined (Level 2)

Comments: CSB has defined and communicated its Data Breach Response Plan, including its processes and procedures for data breach notification.

39. 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, FY 2020 SAOP FISMA Metrics, Sections 9 10, and 11)

Defined (Level 2)

Comments: CSB has defined its privacy awareness training program based on organizational requirements, culture and the types of Personal Identifiable Information and Protected Health Information that its user have access to.

40.1. Please provide the assessed maturity level for the agency's Protect - Data Protection and Privacy program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Data Protection and Privacy, the domain is concluded a "Defined."

## Function 2C: Protect - Data Protection and Privacy

40.2. 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?

**Based on the maturity level of the individual areas within Data Protection and Privacy, the domain is concluded as "Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined." However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.**

## Function 2D: Protect - Security Training

41. To what degree have the roles and responsibilities of security awareness and training program stakeholders been defined, and 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).

Defined (Level 2)

**Comments: The roles and responsibilities for security awareness and training program stakeholders have been defined and communicated across CSB and resource requirements have been established.**

42. 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)?

Defined (Level 2)

**Comments: CSB has defined its process for assessing the knowledge, skills, and abilities of its workforce to determine its awareness and specialized training, and periodically updating its assessment to account for the changing risk environment.**

## Function 2D: Protect - Security Training

43. 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).

Defined (Level 2)

Comments: CSB has implemented and continues to perform organization-wide security awareness and training planning.

44. 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 2021 CIO FISMA Metrics: 2.15; NIST SP 800-50: 6.2; CSF: PR.AT-2; SANS Top 20: 17.4).

Defined (Level 2)

Comments: Processes are in place for tracking completion of security awareness training. This includes employee attestation to completion of the security awareness training and follow-up identify individuals have not completed training requirements.

45. 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 2021 CIO FISMA Metrics: 2.15)?

Ad Hoc (Level 1)

Comments: Specialized security training is normally provided; however, training individuals I specialized IT support areas has not been conducted in the last 12 months.

46.1. Please provide the assessed maturity level for the agency's Protect - Security Training program.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Security Training, the domain is concluded as “Defined.”

46.2. Please provide the assessed maturity level for the agency's Protect function.

Defined (Level 2)

## Function 2D: Protect - Security Training

Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains the Protection function is concluded as "Defined."

46.3. 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?

Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the Protect function is concluded as Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined." However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

## Function 3: Detect - ISCM

47. To what extent does the organization utilize information security continuous monitoring (ISCM) policies and an ISCM strategy that addresses ISCM requirements and activities at each organizational tier (NIST SP 800-37 (Rev. 2) Task P-7; NIST SP 800-137: Sections 3.1 and 3.6)?

Defined (Level 2)

Comments: The CSB Technology Security Plan contains the CSB Information Security Continuous strategy and [policies and identifies how the information security continuous monitoring strategy is communicated for the specified areas.

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; NIST 800-37, Rev. 2 Task P-7 and S-5).

Defined (Level 2)

Comments: CSB has defined the roles and responsibility Information Security Continuous Monitoring.

49. How mature are the organization's processes for performing ongoing information system assessments, granting system authorizations, including developing and maintaining system security plans, and monitoring system security controls (OMB A-130, 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) Task S-5; NIST SP 800-18, Rev. 1, NISTIR 8011; OMB M-14-03; OMB M-19-03)

## Function 3: Detect - ISCM

Defined (Level 2)

Comments: CSB has defined its processes for performing ongoing security controls assessments; granting systems authorizations, including developing and maintaining system security plans; and monitoring security controls for individual systems.

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 2)

Comments: CSB's process for collecting and analyzing ISCM performance measures and reporting findings is systemic and allows, through the use of tools, automatic notification of threats or attempts to exploit attack vectors on CSB network.

51.1. Please provide the assessed maturity level for the agency's Detect - ISCM domain/function.

Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Detect - ISCM, the domain/function is concluded as "Defined."

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?

Based on the maturity level of the individual areas within Detect- ISCM, the domain/function is concluded as Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined." However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

## Function 4: Respond - Incident Response

52. To what extent does the organization utilize an incident response plan to provide a formal, focused, and coordinated approach to responding to incidents (NIST SP 800-53 REV. 4: IR-8; NIST SP 800-61 Rev. 2, section 2.3.2; CSF, RS.RP-1, Presidential Policy Directive (PPD) 8 – National Preparedness)?

Defined (Level 2)

Comments: CSB's incident response policies, procedures, plans, and strategies have been defined and communicated across the organization.

## Function 4: Respond - Incident Response

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; CSF, RS.CO-1, OMB M-20-04; FY 2021 CIO FISMA Metrics: Section 4; CSF: RS.CO-1; and US-CERT Federal Incident Notification Guidelines)?

Defined (Level 2)

Comments: CSB has defined and communicated the structures of its incident response teams, roles, and responsibilities of incident response stakeholders and associated levels of authority and discrepancies.

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-20-04; CSF: DE.AE-1, DE.AE-2 -5, PR.DS-6, RS.AN-1 and 4, and PR.DS-8; and US-CERT Incident Response Guidelines)

Defined (Level 2)

Comments: CSB has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.

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)

Defined (Level 2)

Comments: CSB has developed containment and eradication strategies for each major incident type. In developing its strategies, the organization has taken into consideration the potential damage to and theft of resources, the need for evidence preservation, service availability, time and resources needed to implement the strategy, effectiveness of the strategy, and duration of the solution.

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-20-04; NIST SP 800-53 REV. 4: IR-6; US-CERT Incident Notification Guidelines; PPD-41; CSF: RS.CO-2 through 5; DHS Cyber Incident Reporting Unified Message)

Defined (Level 2)

Comments: CSB has defined its requirements for personnel to report suspected security incidents to the CSB's chief information officer. within CSB's defined time frames. In addition, CSB has defined its processes for reporting security incident information to the United States

## Function 4: Respond - Incident Response

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-20-04; PPD-41).

Comments: CSB has defined its processes and supporting technologies for detecting and analyzing incidents, including the types of precursors and indicators and how they are generated and reviewed, and for prioritizing incidents.

Consistently Implemented (Level 3)

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)

Defined (Level 2)

Comments: CSB has identified and fully defined its requirements for the responses technologies it uses in the specified areas.

59.1. Please provide the assessed maturity level for the agency's Respond - Incident Response domain/function.
Defined (Level 2)

Comments: Based on the maturity level of the individual areas within Respond – Incident Response, the domain/function is concluded as "Defined."

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?

Based on the maturity level of the individual areas within Respond – Incident Response, the domain function is concluded as Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined." However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level

## 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, CP-2, and CP-3; NIST SP 800-34; NIST SP 800-84; FCD-1: Annex B)?

Consistently Implemented (Level 3)

Comments: CSB has identified the roles and responsibilities of stakeholders involved in information systems contingency planning across the organization.

61 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; NIST IR 8286; FIPS 199; FCD-1; OMB M-19-03; FY 2021 CIO FISMA Metrics, Section 5; CSF:ID.RA-4)?

Defined (Level 2)

Comments: CSB uses the results of business impact analyses to guide contingency planning efforts.

62 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 2021 CIO FISMA Metrics: 5.1; OMB M-19-03; CSF: PR.IP-9)?

Defined (Level 2)

Comments: CSB has defined procedures to ensure that processes for information system contingency plan development, maintenance and integration with other continuity areas have been defined and include the following phases: activation and notification recovery, and reconstitution.

63 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 2021 CIO FISMA Metrics, Section 5; CSF: ID.SC-5 and CSF: PR.IP-10)?

Ad Hoc (Level 1)

Comments: CSB has not defined processes for information system contingency plan testing and exercises.

64 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 2021 CIO FISMA Metrics, Section 5; and NARA guidance on information systems security records)?

## Function 5: Recover - Contingency Planning

Defined (Level 2)

Comments: The organization has defined procedures to ensure that CSB performs information system backup and storage, including use of alternate storage and processing sites. CSB has not defined processes for information system contingency plan testing and exercises.

65 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)?
Defined Level 2)

Comments: CSB has defined procedures to 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.

66.1. Please provide the assessed maturity level for the agency's Recover - Contingency Planning domain/function.
Defined (Level 2)

Comments Based on the maturity level of the individual areas within Recover – Contingency Planning, the domain/function is concluded as "Defined."

66.2. 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?
Based on the maturity level of the individual areas within Respond – Incident Response, the domain function is concluded as Defined". We limited our testing to those questions with criteria added to the metric that would materially change our FY2020 response. For those metrics whose policies, procedures, and strategies were documented, we rated the CSB at Level 2, "Defined." However, we did not test to determine what additional steps the Agency needs to complete to achieve a higher maturity level.

## APPENDIX A: Maturity Model Scoring

A.1. Please provide the assessed maturity level for the agency's Overall status.

**Function 1A: Identify - Risk Management**

| Function | Count |
|---|---|
| Ad-Hoc | 2 |
| Defined | 8 |
| Consistently Implemented | 0 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Define (Level 2)**

**Function 1B: Identify - Supply Chain Risk Management**

| Function | Count |
|---|---|
| Ad-Hoc | 4 |
| Defined | 0 |
| Consistently Implemented | 0 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Ad Hoc (Level 1)**

**Assessed Rating: Ad Hoc (Level 1)**

## APPENDIX A: Maturity Model Scoring

**Function 2A: Protect - Configuration Management**

| Function | Count |
|---|---|
| Ad-Hoc | 2 |
| Defined | 6 |
| Consistently Implemented | 0 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

**Function 2B: Protect - Identity and Access Management**

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 6 |
| Consistently Implemented | 2 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

## APPENDIX A: Maturity Model Scoring

**Function 2C: Protect - Data Protection and Privacy**

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 5 |
| Consistently Implemented | 0 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

**Function 2D: Protect - Security Training**

| Function | Count |
|---|---|
| Ad-Hoc | 1 |
| Defined | 4 |
| Consistently Implemented | 0 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

## APPENDIX A: Maturity Model Scoring

**Function 3: Detect - ISCM**

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 3 |
| Consistently Implemented | 1 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

**Function 4: Respond - Incident Response**

| Function | Count |
|---|---|
| Ad-Hoc | 0 |
| Defined | 6 |
| Consistently Implemented | 1 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

## APPENDIX A: Maturity Model Scoring

**Function 5: Recover - Contingency Planning**

| Function | Count |
|---|---|
| Ad-Hoc | 1 |
| Defined | 4 |
| Consistently Implemented | 1 |
| Managed and Measurable | 0 |
| Optimized | 0 |

**Calculated Rating: Defined (Level 2)**

**Assessed Rating: Defined (Level 2)**

## APPENDIX A: Maturity Model Scoring

### Overall

| Function | Calculated Maturity Level | Assessed Maturity Level | Explanation |
|---|---|---|---|
| Function 1: Identify - Risk Management / Supply Chain RiskManagement | Defined (Level 2) | Defined (Level 2) | Based on the maturity level of the individual areas within the Risk Management and Supply Chain Risk Management domains, the overall maturity level of the Identify function is concluded as “Defined”. |
| Function 2: Protect - Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training | Defined (Level 2) | Defined (Level 2) | Based on the maturity level of the individual areas within the Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training domains, the overall maturity level of the Protect function is concluded as “Defined”. |
| Function 3: Detect - ISCM | Defined (Level 2) | Defined (Level 2) | Based on the maturity level of the individual areas within Detect - ISCM, the overall maturity level of the domain/function is concluded as “Defined.” |
| Function 4: Respond - Incident Response | Defined (Level 2) | Defined (Level 2) | Based on the maturity level of the individual areas within Respond – Incident Response, the overall maturity level of the domain/function is concluded as “Defined.” |
| Function 5: Recover - Contingency Planning | Defined (Level 2) | Defined (Level 2) | Based on the maturity level of the individual areas within Recover – Contingency Planning, the overall maturity level of the domain/function is concluded as “Defined.” |
| Overall | Not Effective | Effective | The U.S. Chemical Safety and Hazard Investigation Board’s Information Security Program has demonstrated that it has defined policy, procedures, and strategies for all five of its Information security function areas. |

**Appendix B**

# *Status of CSB Corrective Actions for FY 2018, FY 2019, and FY 2020 FISMA Report Recommendations*

The table below describes the recommendations from previous FISMA evaluations that remained unimplemented as of February 2021.

| OIG Report | Recommendation | | Corrective action | OIG analysis of corrective action status |
|---|---|---|---|---|
| *CSB Still Needs to Improve Its 'Incident Response' and 'Identity and Access Management' Information Security Functions*, Report No. 19-P-0147 | 1 | Define and implement processes for the use of Personal Identity Verification cards for logical access. | Multifactor authentication has been implemented for all Virtual Private Network users. | Completed in FY 2021. |
| *CSB's Information Security Program Is Not Consistently Implemented; Improvements Are Needed to Address Four Weaknesses*, Report No. 21-E-0071 | 2 | Complete the risk assessment process as required by National Institute of Standards and Technology 800-37, reevaluate the Risk Management Framework to make it more fluent to leverage day-to-day processes in place for completing the risk assessment, and determine how to best implement an organizationwide governance process for monitoring and reporting on risks. | Based on a follow-up discussion with CSB information technology management, while a risk assessment process is in place, one has not been performed since FY 2020 due to the coronavirus pandemic.<br><br>In addition, due to the size and resources of the organization, processes related to governance and process management are handled through manual processes. There is no automated solution that provides a centralized, enterprisewide view of cybersecurity risks across the organization. However, there are documented procedures in place for implementing an organizationwide governance process for monitoring and reporting risks. | Corrective action in process.<br><br>Planned completion date is FY 2022. |
| | 3 | Document the process in place to monitor required flaw remediation to resolution and enhance the flaw remediation process to require approvals if risks cannot be mitigated to an acceptable level in a timely manner. In addition, develop | The CSB has implemented an information technology Plans of Actions & Milestones tracking sheet with a defined time frame for remediating security weaknesses; however, there is not a documented procedure in place that defines how the tracking sheet will be used to | Corrective action in process.<br><br>Planned completion date is FY 2022. |

| OIG Report | Recommendation | | Corrective action | OIG analysis of corrective action status |
|---|---|---|---|---|
| | | time frames and monitoring on the timeliness of applying patch updates. | mitigate any security weakness identified. | |
| | 4 | Implement a process to ensure that privacy awareness training is provided to all individuals, including role-based training where needed. | The CSB has developed and provided annual privacy awareness training to all employees. | Completed in FY 2021. |
| | 5 | Implement information security awareness and specialized security training policies and procedures to provide exposure to areas specific to individuals that have a role in supporting information security or technology-related areas. In addition, document an information security awareness and training strategy that leverages its organizational skills assessment and factors the training program priorities, funding, the goals of the program, and targeted audiences. | Based on discussions with the CSB information technology management, specialized security training is normally provided; however, training for individuals in specialized information technology support areas has not been conducted since FY 2020. | Corrective action in process.<br><br>Planned completion date is FY 2022. |
| | 6 | Perform disaster recovery testing on an annual basis. In addition, evaluate alternate methods to store backup media off-site. | Processes for information system contingency plan testing and exercises have not been defined. Contingency plan tests for systems are performed in an ad-hoc, reactive manner due to the impact of coronavirus pandemic and lack of resources.<br><br>Additionally, based on discussions with the CSB information technology management, the backups are not being consistently rotated off-site. | Corrective action in process.<br><br>Planned completion date is the third quarter of FY 2022. |

Source: OIG analysis of CSB corrective actions. (EPA OIG table)

**Appendix C**

# *CSB Response to Report*

**U.S. Chemical Safety and Hazard Investigation Board**

1750 Pennsylvania Avenue NW, Suite 910 | Washington, DC 20006
Phone: (202) 261-7600 | Fax: (202) 261-7650
www.csb.gov

**Honorable Katherine A. Lemos**
Chairman and CEO

March 9, 2022

Re: Draft IRM Contractor Produced Report

The CSB welcomes the opportunity to improve upon areas vulnerable to exploitation and thanks the audit staff for their work in these areas.

The CSB concurs with the first recommendation and has approved and published a Vulnerability Disclosure Policy to the CSB website in accordance with the recommendation for improvement. A VDP will provide ethical hackers instruction on how to report vulnerabilities that they have identified and promote cooperation between internal and external stakeholders pertaining to vulnerabilities.

The CSB also concurs with the second recommendation regarding the need improve its cybersecurity program by consistently storing system backups at an offsite location a sufficient distance from its headquarters. Offsite manual backup procedures have resumed, a new agency purchasing officer has joined the agency and has conducted preliminary market research, and the CSB is currently undergoing a survey to understand our needs for cloud services. The anticipated goal date for award is 30 June 2022 with realized outcomes by 15 July 2022.

David LaCerte
Senior Advisor and Executive Counsel

**Appendix D**

# *Distribution*

Chairperson and Chief Executive Officer
Senior Advisor and General Counsel
EPA OIG Liaison
Information Technology Director/Chief Information Officer