Initial Performance Summary

American Battle Monuments Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	1	3	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	5	4	8
Multiple Attack Vectors	0	0	0
Total	**6**	**7**	**9**

CIO Self-Assessment

During FY21 ABMC has made significant progress on consolidating all its systems and moving them to a single cloud based infrastructure. Now all of its major systems, serving its public mission have been migrated a the new Cloud service.

The pandemic has introduced unique challenge which ABMC has tackled head-first by implementing a FEDRAMP Secure Access Service Edge Solution and phased out its legacy VPN technology. This allowed to ensure continued operations while improving security posture by fully leveraging managed security services.

Independent Assessment

Overall ABMC has an effective information security program in place that not only addresses FISMA requirements, but also meets the business needs of ABMC. ABMC has made significant improvements in its overall information security, as measured in FISMA, and has raised all functional areas to managed and measurable. However, we make several recommendations to ABMC that can further strengthen and improve its information security.

Initial Performance Summary

Advisory Council on Historic Preservation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	At Risk	N/A
Detect	Managing Risk	N/A
Respond	At Risk	N/A
Recover		N/A
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

Legacy end of support systems were a significant concern. The ACHP had to take a mutli-year phased approach to replace these systems due to budget constraints. These systems have been actively replaced or upgraded (with HVA systems prioritized) in FY 2021. Upgrades and replacements will continue into FY 2022.

The shift to a maximum teleworking workforce presented challenges, however we were prepared to use modern zero trust/SDN technologies to provide secure access. This allowed a smooth transition to a remote workforce while providing secure access.

Due to proactive monitoring and implementation of improved cybersecurity detection, visibility, and remediation capabilities no successful major or minor incidents have occurred.

Independent Assessment

Initial Performance Summary

Administrative Conference of the United States

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	NA	0	0
E-mail	NA	0	0
External/Removable Media	NA	0	0
Impersonation	NA	0	0
Improper Usage	NA	0	0
Loss or Theft of Equipment	NA	0	0
Web	NA	0	0
Other	NA	0	0
Multiple Attack Vectors	NA	0	0
Total		**0**	**0**

CIO Self-Assessment

ACUS has implemented MFA for email and accessing sensitive data. Vulnerability audits are performed quarterly and vulnerabilities are then addressed by implementing the fixes needed. This includes patching to all network devices and replacement of hardware that is outdated and a security risk.

Independent Assessment

There's annual auditing in place for all systems to confirm there are no vulnerabilities to the entire network. If there are any vulnerabilities found, the necessary actions are then taken to fix the vulnerability.

Initial Performance Summary

African Development Foundation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	2
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**2**

CIO Self-Assessment

The United States African Development Foundation (USADF has developed a risk management governance that is demonstrated through the implementation and maintenance of a risk management structure that addresses the organization-wide risk management strategy. USADF strives to mitigate cybersecurity risks by implementing through its leadership an organization- wide enterprise risk management plan, remaining compliant by participating in DHS's CDM program. USADF performs an annual security and risk assessment on its information system resources according to the NIST Standard Publication guidelines and in compliance with FISMA. USADF has equally outsourced cybersecurity risks by moving critical assets to US government shared services and to FedRAMP approved cloud services providers. USADF has implemented DHS mandated EINSTEIN 3A DNS sink-holing and Cloud Email filtering as part of its effort to mitigate and reduce cybersecurity risk exposure. USADF has implemented zero-trust architecture for remote access to applications internal and external to its users. Even though USADF has embraced these efforts in managing risks, challenges still exist.

USADF has implemented a Risk Management Plan that covers risk management of all USADF information system resources which are categorized based on the business function, threat exposure, vulnerabilities and data type. Strategies for risk remediation are proportionate to the risks to the information system resources. The major constraints in resolving or mitigating risks are budgets and human resources. Senior management is addressing these constraints to make cybersecurity risk management and mitigation a priority at USADF.

USADF's senior management is fully engaged in reviewing risk analysis results and reports and supports the ongoing

Independent Assessment

USADF's information security program was evaluated as part of the FY2021 FISMA Audit, which was conducted by CliftonLarsonAllen LLP (CLA). This audit included an evaluation of a sample of 4 of 11 USADF internal and external information systems in USADF's FISMA inventory as of February 17, 2021. The FY2021 FISMA Audit noted that USADF implemented an effective information security program and practices by achieving an overall Optimized maturity level based on the FY 2021 IG FISMA Reporting Metrics. There were a few recommendations made to help USADF improve their information security program. These recommendations can be found in the FY2021 FISMA Audit report.

efforts of USADF's cybersecurity risk management strategy and processes. USADF's CISO ensures active involvement of information system owners, common control providers, CIOs, senior managers, designate

Initial Performance Summary

Armed Forces Retirement Home

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

AFRH’s mission and strategy is to provide residences and related services for retired and former members of the Armed Forces. As a “defend in place” continuing care facility their core responsibility is the care and safety of their residents and personnel. The objective of the Security Program is to create effective administrative, technical and physical safeguards in order to protect critical data and resources. The Armed Forces Retirement Home (AFRH) in coordination with the Department of Interior – Office of the Chief Information Officer (DOI-OCIO) continues to strive to improve the organization's security posture by ensuring the correct technologies and security controls are in place that reduce the organization’s risk, as well as processes to monitor the effectiveness of the security program. AFRH continues to improve in areas such as continuous monitoring, risk identification and management and security documentation development. AFRH will continue in coordination with DOI to: identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems; assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks.

Independent Assessment

The Armed Forces Retirement Home (AFRH) in coordination with the Department of Interior – Office of the Chief Information Officer (DOI-OCIO) continue to strive to improve the organization's security posture by ensuring the right technologies and security controls are in place that reduce the organization’s risk, as well as processes to monitor the effectiveness of the security program. AFRH’s main mission and strategy is to provide residences and related services for retired and former members of the Armed Forces. As a “defend in place” continuing care facility their core responsibility is the care and safety of their residents and personnel.

The objective of the Security Program is to create effective administrative, technical and physical safeguards in order to protect critical data and resources. DOI conducts an annual risk assessment on the AFRH program policies and general support system to identify security weaknesses consisting of technical testing, interviews and observation techniques. The assessor analyzes all assessment results to provide the AFRH and the AOs with an assessment of the security and privacy controls that safeguard the Confidentiality, Integrity, and Availability (CIA) of data hosted by the system as described in the AFRH System Security Plan (SSP). The assessment seeks to verify and validate the following:

- If the system is compliant with NIST 800-53 rev4;
- If the underlying infrastructure supporting the system is secure;
- If the system and data are securely maintained; and
- If proper configuration associated with the database and file structure storing the data are in place.

Planned activities:

- Identify, assess and document Supply Chain Management policy and procedures

AFRH continues to refine their security practices in alignment with FISMA and other federal regulatory policy to mature their security program and practices.

Initial Performance Summary

Barry Goldwater Scholarship and Excellence in Education Foundation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	At Risk	Ad Hoc
Respond	Managing Risk	Ad Hoc
Recover		Ad Hoc
Overall	At Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

Prior to COVID-19, both BGSF employees were already telework capable with security measures in place. The transition to 100% telework only increased the frequency of telework. Effective Oct 1, 2020, BGSF permanently transitioned to 100% telework for all operations.

Independent Assessment

The Barry Goldwater Foundation is a small agency with two permanent employees. It does not have in-house IG or CIO. There are five computers and two printers and no mobile devices. We do not have any HVAs. The Foundation's IT systems are not connected to any government computer network. The computers password protected, all data is encrypted at rest and in transit, and all data is backed up daily. With only 2 users, the agency does not distinguish between privileged vs. non privileged users and we are not issued PIV cards. The agency coordinates with GSA, USDA OCFO, DOI/IBC, contracted IT support, and the website/program coordinator, regarding operating systems and PII security. Both BGSF employees are aware of their responsibilities with respect to data security and PII. While the agency has not had an incident, the agency IT contract provides for on-site support should an incident occur.

Initial Performance Summary

Commission on Civil Rights

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

USCCR relies extensively on IT resources to accomplish its mission. The overall FY 2021 FISMA maturity score for USCCR's security program is Consistently Implemented. The USCCR maturity score for FY 2020 was also Consistently Implemented. However, USCCR continues to take positive steps for improving its security posture. USCCR made some improvements in the agency's IT Modernization plan. USCCR upgraded its legacy network and added tools to assist in becoming fully compliant with BODs and Emergency Directives. USCCR has a similar risk profile to other small, internet enabled agency's that have had significant success adopting cloud-based services. USCCR continues to attempt to align its IT strategy with OMB and the President Management Agenda's focus on utilizing interagency shared services, cloud SaaS and IaaS models. USCCR acknowledges that it must reduce its unsupported software to remove the vulnerabilities and better management of non-standard use software. Amid the pandemic USCCR still met its goals to implement the IT Modernization Plan. The agency strengthened its VPN and made progress implementing all staff with Windows 10 platforms and to move past the unsupported Windows 7 endpoints. As a result In FY2021, hopes to continue the IT Modernization Plan to increase its maturity.

Independent Assessment

To meet FISMA requirements USCCR contracted with an independent auditor to conduct the FY 2019 independent evaluation of its information security program and practices as a performance audit under Generally Accepted Government Auditing Standards. The auditors concluded that overall, USCCR has invested significantly to ensure that its information security policies and procedures comply with FISMA requirements and recommendations made over the past year. The agency has developed several plans of action and milestones (POA&Ms) to address FISMA requirements the continued items that are at risk or higher. The scope of the evaluation included all aspects of USCCR's IT environment. Overall USCCR's information security program is effective but can be improved upon. The primary reason for the "consistently implemented" state of USCCR's information security program is based on weaknesses found in the areas of Identify, Protect, and Respond. The state would have "managed and measurable" if the agency was to obtain the resources to fully implement the security program. The primary recommendation is to address the POA&Ms already identified and to ensure that the policies and procedures outlined in the POA&Ms is successfully addressed in FY2021

Initial Performance Summary

Commission of Fine Arts

Framework	CIO Rating	IG Rating
Identify	At Risk	N/A
Protect	High Risk	N/A
Detect	At Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	**At Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	2
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**2**

CIO Self-Assessment

While progress is being made in implementing basic cybersecurity solutions, (e.g. updated MTIPS, E3A, CDM and the ability to more efficiently manage hardware assets), the greatest cybersecurity risk to the agency remains the absence of knowledgeable and dedicated IT and cybersecurity staff, or access to such staff in other agencies, with the capacity and expertise to fully address the CFA's cybersecurity infrastructure.

Independent Assessment

Initial Performance Summary

Consumer Financial Protection Bureau

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	0	0
Loss or Theft of Equipment	100	57	101
Web	0	0	4
Other	0	7	0
Multiple Attack Vectors	1	0	0
Total	**104**	**64**	**105**

CIO Self-Assessment

Since its inception, CFPB has taken an innovative approach to fulfill its mission to serve the American consumer by continuing to leverage digital and cloud technologies. While the journey to becoming a modern agency has presented opportunities for efficiency, it has not come without challenges. CFPB uses internal security controls assessments, continuous monitoring, advanced technical capabilities, innovative security training, and audits to identify cyber risks and opportunities to gain efficiencies in operations that enhance mission effectiveness and reduce risk. The results of these activities are further analyzed to help inform decisions that consider the following: Enhancing visibility into the data and assets that need to be protected in a distributed IT environment in a way that embraces the shared service models of FedRAMP and federal service providers; Establishing cybersecurity supply chain risk management processes; Addressing the data protection needs of the organization focused on the most valuable IT assets, while not hindering CFPB's ability to interface with the public or limiting the mission to ensure fairness in the financial marketplace; Achieving near real-time situational awareness to cyber threats and vulnerabilities; Implementing multifactor authentication on all CFPB GFE, and Safeguarding sensitive information from misuse, while also making the appropriate data available to carry out CFPB's mission. As a result of the COVID-19 pandemic, the digital, teleworking workforce has grown, resulting in increased exposure to phishing, and malware. To address this risk, CFPB implemented targeted phishing simulations and increased the enforcement of cybersecurity training compliance. The network accounts of non-compliant employees are blocked when they do not complete their mandatory training on time. CFPB has also published articles weekly to communicate the latest phishing

Independent Assessment

Overall, we found that the Bureau's information security program is operating effectively at a level-4 (managed and measurable) maturity. For instance, the Bureau's information security continuous monitoring and security training processes are effective and operating at a level 4. However, we identified further opportunities to strengthen processes and controls in the area of risk management and configuration management to ensure that its information security program remains effective. Our 2021 FISMA audit report includes 3 recommendations to strengthen controls in these areas.

and cybersecurity threats, disaster-themed scams, etc.

Initial Performance Summary

Commodity Futures Trading Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	2	1	0
Web	0	0	0
Other	2	1	0
Multiple Attack Vectors	0	0	0
Total	**4**	**3**	**0**

CIO Self-Assessment

The risk landscape and external influences are rapidly changing as COVID-19 continues to present new challenges. Cybersecurity is one of the most important issues facing our markets and clearing organizations today, in terms of financial stability and market integrity. Cyber attacks are on the rise with sophisticated tactics using a combination of hacking, malware, and social engineering. CFTC's cybersecurity program is prepared for the growing threat landscape, with policies and compliance activities that govern the protection of our information, assets and mission functions. Because technology-driven innovation enhances our overall mission, solid cybersecurity and information-security practices must safeguard our systems' underpinning technologies. The E.O. 14028 has allowed the Commission to apply for funding to expedite and implement key security services. The TMF program will allow the Commission to:
•Implement a Zero Trust Framework.
•Develop a PII data protection program to include DLP capability.
•Implement Endpoint Detection & Response technology.
Other areas of risks related to internal controls include improve contingency planning activities to lower the risk of data loss, and strengthen the Commission's vulnerability management program. CFTC will continue to develop an insider threat program, and maintain a safe and secure telework operating environment during the pandemic by leveraging the Interim Telework Guidance published by CISA. The impacts of added requirements from the E.O and the current threat landscape require that we continue to examine the effects and apply best practices to provide timely, reliable, and secure IT services during these unprecedented times. Our cybersecurity program requires a commitment in the investment of people, processes, technology, and capital to

Independent Assessment

We rated the Commodity Futures Trading Commission information security program as “Effective,” and note there are opportunities to optimize the program as detailed in our recommendations, namely: integrating risk management into an Enterprise Risk Management (ERM) program , re-evaluate the flaw remediation process which involves tracking and managing medium to critical vulnerabilities that have not been remediated within the prescribed time frame, and address a deficiency in privacy office for out-of-date policies and procedures to effectively respond to major breaches.

provide information assurance and computer network defense for our mission critical systems and data.

Initial Performance Summary

Council of the Inspectors General on Integrity and Efficiency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	Managing Risk	N/A
Detect	Managing Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

CIGIE has taken the following steps towards improving our security posture and reaching FISMA compliance. The following are the most significant achievements.

- CIGIE is almost done deploying all HSPD-12 related technologies required to meet this mandate.
- CIGIE has upgraded non-FISMA Wi-Fi infrastructure to incorporate FIPS140-2 compliant only equipment.
- CIGIE has upgraded all network switches to FIPS140-2 fully managed equipment.
- CIGIE has upgraded all network firewalls to FIPS140-2 fully managed equipment.
- CIGIE has implemented a more advanced authentication of guest Wi-Fi devices.
- CIGIE has improved its log collection and auditing capabilities enhancing visibility or anomalous behaviors.
- CIGIE has enhanced its MDM capabilities by adding additional controls to laptops.
- CIGIE has joined the DHS EINSTEIN 1, 2, and 3a.
- CIGIE has decommissioned its Windows 2008 R2 domain controllers to Windows 2019 Server.
- CIGIE has implemented pre-logon VPN and security services.
- CIGIE has implemented Network Access Control, specifically, rogue device identification and isolation.

Independent Assessment

N/A

Initial Performance Summary

Corporation for National and Community Service

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	5	1
Loss or Theft of Equipment	0	2	3
Web	0	0	0
Other	3	5	5
Multiple Attack Vectors	0	0	0
Total	**6**	**12**	**9**

CIO Self-Assessment

AmeriCorps has taken a series of actions to address certain security risks that have continued during the COVID-19 pandemic. AmeriCorps continues testing full scale telework program to verify user functionality and systems environment capabilities. Regarding PIV for authentication, AmeriCorps has currently relaxed PIV enforcement policy for new users and for employees with damaged or unusable cards, as replacement card locations were not operational due to the COVID-19 pandemic. Focusing on these key areas allowed AmeriCorps to make significant improvements to our cybersecurity program, shifting our risk management rating from “At Risk” to “Managing Risk” across all five functions. AmeriCorps rigorously enforced multifactor authentication procedures across the enterprise. This helped reduce risk in the identify function area by reducing the use of username/password and ensuring that only authorized users could access information being sought. AmeriCorps’ cybersecurity program is currently taking strategic measures to enforce PIV authorization and align with OPM guidance on federal return to workforce procedures. AmeriCorps will continue to take necessary steps to protect vital information that helps us achieve our mission.

Independent Assessment

AmeriCorps’s information security program was evaluated as part of the FY2021 FISMA Evaluation. This evaluation included a review of four AmeriCorps internal and external information systems. The FY2021 FISMA Audit noted that AmeriCorps’ information security program is NOT EFFECTIVE, because the five FISMA security function areas in its information security program and practices have not achieved sufficient maturity based on the FY 2021 IG FISMA Reporting Metrics. AmeriCorps was rated at a Defined maturity level. The control weaknesses that continue to prevent AmeriCorps from maturing its cybersecurity program relate to the following DHS IG metrics in the Identify, Protect, and Detect function areas:

- Organization-wide risk management strategy,
- IT asset inventory management,
- Standard baseline configurations,
- Personal Identify Verification (PIV) multifactor authentication, and
- Vulnerability and patch management program.

In addition, controls weaknesses noted this year in the Respond and Recover function areas include the lack of conducting an incident response test, and not performing disaster recovery testing for two key systems.

To address the continuing weaknesses in AmeriCorps’ information security program and practices, we added 13 new recommendations to the 31 unimplemented recommendations from prior years. Implementing these recommendations will assist AmeriCorps in addressing challenges in its development of a mature and effective information security program. These recommendations can be found in the FY2021 FISMA Evaluation report.

Initial Performance Summary

Consumer Product Safety Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Consistently Implemented
Recover		Ad Hoc
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	3	0
Loss or Theft of Equipment	1	0	1
Web	0	0	0
Other	1	2	1
Multiple Attack Vectors	0	0	0
Total	**5**	**5**	**3**

CIO Self-Assessment

The Consumer Product Safety Commission (CPSC) has worked throughout the past year to advance protections for agency information and systems. Like many other agencies, the CPSC was concerned about increased threats from ransomware attacks. Agency management reviewed the recommendations stipulated within CISA's ransomware guidance (AA21-131A) and determined that 7 of the 11 recommendations are already fully implemented within the CPSC computer environment; two are partially implemented; and two are currently being assessed. Additionally, the IT security staff performed routine IT security operations while also implementing new programmatic and technological improvements to reduce agency cyber risk.

Accomplishments for the past year include:

- Implemented MTIPS block rule for all inbound critical and high security threats. This resulted in a significant drop in the amount of malicious traffic reaching the CPSC network.
- Significantly expanded the use of data logging and aggregating tools–which helped to improve overall awareness of agency's security posture.
- Implemented requirements from the DHS Binding Operational Directive 20-01, which required all federal agencies to develop and publish a Vulnerability Disclosure Policy (VDP).
- Implemented CISAs Web Application Scanning (WAS) shared service.
- Implemented the DHS Continuous Diagnostics & Mitigation (CDM) infrastructure.
- Provided simulated phishing and ransomware training to all agency employees.

Independent Assessment

We evaluated the CPSC's information security program's policies, procedures, and practices as a whole and tested the effectiveness of CPSC's security policies, procedures, and practices of a representative sample of its information systems.

Our evaluation found that the CPSC continues to make progress in implementing the FISMA requirements. For example, the CPSC has closed five recommendations included in the FY 2020 FISMA report; implemented a new tool for identifying deviations from common secure configurations; began the final phases of implementing a tool to assist with privileged user account management; developed procedures and implemented safeguards to prevent DNS infrastructure tampering; updated security training and role-based training procedures; updated the ISCM plan and defined system-level performance metrics for configuration settings, vulnerability management, security impact analysis, and authorization to operate; migrated to a new SIEM tool for log aggregation analysis and alerting; and completed ISCP testing for the two of its major systems.

However, we determined that the CPSC has not implemented an effective information security program in accordance with FISMA requirements. The CPSC has not implemented an effective program because the CPSC has not established a formal approach to information security risk management and has not adequately defined and implemented a process to deploy its limited resources. The CPSC must continue to prioritize the improvement of its information security program in order to achieve an effective information security program. As a result of the evaluation, we made 47 recommendations that the CPSC must address to mature its information security program.

CPSC has made consistent progress in addressing gaps in its information security policies, procedures, and practices with a far more secure environment than just a few years ago. Sustained leadership commitment to IT security has been instrumental in this progress. Challenges remain for CPSC and important work is underway to address the most significant areas of risk.

Initial Performance Summary

Court Services and Offender Supervision Agency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At Risk	Defined
Detect	Managing Risk	Consistently Implemented
Respond	At Risk	Optimized
Recover		Consistently Implemented
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	0	2
Multiple Attack Vectors	0	0	0
Total	**3**	**0**	**2**

CIO Self-Assessment

Cybersecurity continues to be one of the Agency's top priorities. In accordance with Office of Management and Budget and Department of Homeland Security requirements, the Court Services and Offender Supervision Agency (CSOSA) is accelerating its cybersecurity activities around protecting the mission. The Agency is focused on strengthening its security posture and defending against attacks on sensitive law enforcement, national security, and U.S. government personnel data, while maintaining the confidentiality, integrity, and availability of mission systems. The Agency continues to make significant progress in managing information risk and securing our systems, and must continually invest in our cybersecurity capabilities to be effective. In response to the Coronavirus pandemic, CSOSA increased telework for all employees and contractors while continuing to secure its remote access capabilities with Multi Factor Authentication for network access and mitigate risk to the confidentiality, integrity and availability of CSOSA systems.

Independent Assessment

During fiscal year 2021, the Department of Justice (Department) Office of the Inspector General (OIG) reviewed the information security program for the Court Services and Offender Supervision Agency (CSOSA) and the Pretrial Services Agency for the District of Columbia (PSA) (Agency) and one selected system. As a result of our review, the OIG determined that the maturity level for the Agency's information security program is "Level 2 – Defined" for the Security Function: Protect; "Level 3 – Consistently Implemented" across three Security Functions: Identify, Detect, and Recover; and "Level 5 – Optimized" for the Security Function: Respond. Therefore, the OIG determined that one of the five Security Functions: Respond, is effective. However, the OIG determined that the Agency's overall information security program is not effective due to the exceptions noted within the four Security Function areas of Identify, Protect, Detect, and Recover. The Agency should implement our recommendations specifically within the Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, and Contingency Planning metrics of the Identify, Protect, Detect, and Recover Functions to improve the effectiveness of the Agency's information security program.

Initial Performance Summary

Denali Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	At Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	At Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

No High Value Assets

Independent Assessment

The reason it was assessed at this level is because this is a micro-agency not previously subject to all of the requirements of FISMA. It is not effective because the overall level is Defined. The agency has improved from ad hoc to defined in one fiscal year.

Initial Performance Summary

U.S. International Development Finance Corporation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	1	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	0
Loss or Theft of Equipment	10	5	5
Web	0	0	0
Other	0	2	1
Multiple Attack Vectors	0	0	0
Total	**11**	**8**	**7**

CIO Self-Assessment

DFC conducted maturity assessment of the cybersecurity program to identify any gaps and develop a roadmap.
DFC established an agency-wide enterprise risk management program.

Independent Assessment

DFC's information security program was evaluated as part of CLA's FY2021 FISMA Audit. This audit included an evaluation of three FISMA reportable systems at DFC. This along with the maturity of DFC's information security program led to the determination of DFC having an overall effective information security program. There were a few recommendations made to help DFC improve their information security program. These recommendations can be found in the FY2021 FISMA Audit report.

Initial Performance Summary

Department of Homeland Security

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	1	2
E-mail	93	311	25
External/Removable Media	10	17	1
Impersonation	0	0	0
Improper Usage	544	121	522
Loss or Theft of Equipment	15	10	0
Web	30	41	11
Other	379	204	1,241
Multiple Attack Vectors	0	0	5
Total	**1,072**	**705**	**1,807**

CIO Self-Assessment

DHS aims to lead the Federal government by example when it comes to cybersecurity practices and the Administration's priorities. DHS has made significant strides in all four cybersecurity framework functions, Identify, Protect, Detect and Respond & Recover. DHS has achieved the maximum rating of "Managing Risk" for the first time in all four functions required by the Federal Information Security Management Act (FISMA). To overcome cybersecurity risks, DHS actively monitors the Authority to Operate (ATO) status of all FISMA systems with the DHS CIO continuing to focus on resolving expired ATOs and closing high risk Plans of Action & Milestones (POA&M). In addition, significant reductions have been made in enterprise-wide cybersecurity risks and magnitude by standardizing toolsets for the management of mobile assets. Authorization management has been improved by working intensively to support Component success and leveraging situational awareness. Moreover, risks and issues are highlighted in monthly cybersecurity reports where every Component is directed and assisted to mitigate risks and close vulnerabilities. Recent attacks on government and industry have made it clear that despite practicing good FISMA compliance, adversaries are willing and able to carry out sophisticated, well planned, targeted attacks to achieve their goals. As a result, DHS accelerated its Cyber Supply Chain Risk Management implementation efforts and has established a Unified Cybersecurity Maturity Model (UCMM) to appropriately identify and address cybersecurity gaps. DHS is migrating to a Zero Trust Architecture while conducting risk-based and outcome driven FISMA certifications. Furthermore, DHS has offered cybersecurity staffing incentives since FY20 and is establishing the new Cyber Talent Management System to address DHS's historical and ongoing challenges recruiting and retaining individuals with

Independent Assessment

An official from the Department's Office of the Chief Information Security Officer stated that the Department faced significant challenges this year, as its resources were diverted for critical SolarWinds response and recovery efforts. Although, under this year's OIG FISMA reporting metrics, we rated the Department's information security program as "ineffective," it achieved "Level 3 - Consistently Implemented" in three of the five functions. Specifically, the Department earned a maturity rating of "Level 4 - Managed and Measurable" in one function, "Level 3 - Consistently Implemented" in three functions, and "Level 2 - Defined" in one function. DHS components can improve the effectiveness of their information security program by consistently executing the Department's policies, procedures, and practices. For example, we identified (1) systems without authority to operate; (2) known information security weaknesses not being mitigated timely; (3) security patches that were not applied timely to mitigate critical and high-risk security vulnerabilities on selected workstations and network equipment; and (4) an unsupported operating system on one component's network equipment. Since 2019, our independent contractor has performed fieldwork at nine selected components and rated four components' information security programs as "ineffective." Finally, DHS has not yet incorporated new and revised security controls from applicable NIST publications, such as NIST SP 800-37 Rev 2's seven-step RMF process in its ongoing authorization process. In some cases, DHS' policies contradict which NIST publication should be in use. (Note that our overall self-assessment rating does not include the US Coast Guard, or the results from Function 1B on Supply Chain Risk Management.)

the skills necessary to execute DHS's cybersecurity mission.

Initial Performance Summary

Defense Nuclear Facilities Safety Board

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	3	1	0
Web	0	0	0
Other	1	0	3
Multiple Attack Vectors	0	0	0
Total	**4**	**1**	**3**

CIO Self-Assessment

The most pressing cybersecurity challenges faced by the DNFSB continues to be recruiting and retaining a cybersecurity workforce (both federal and contractor) with adequate cybersecurity expertise, ensuring the DNFSB has the appropriate mix of continuous monitoring tools to monitor the implementation of security controls for all system components (and that the tools are being properly used), and ensuring that agency documentation is updated on a timely manner to reflect the implementation of new tools and changes to processes.

DNFSB has appointed a new Chief Information CISO, has awarded a new IT support contract with additional cybersecurity staff, and has put the tools provided by CISA under the CDM Defend F offering (the CDM Agency Dashboard and underlying tools) into production. In addition, the DNFSB is implementing a number of additional cloud-based security tools that will provide greater insight and protection of both the DNFSB's internal system and the cloud-based systems (email, collaboration, etc.) that are most critical to the agency's mission.

Independent Assessment

Most of the IG FISMA metric and maturity level indicators for each metric are directed to large agencies with the resources and risk that would require that they meet level four (4) maturity to be effective. Due to the small organizational structure, The DNFSB can operate and communicate more efficiently and effectively compared to larger Federal agencies. The DNFSB's key risk management personnel are intimately involved in all aspects of The DNFSB's information security program and are aware of every important decision involving risk to the Agency's information system, information, and mission. The DNFSB should continue to formalize its information security program by fully developing documenting standard operating procedures for security controls in place to manage the risk to the DNFSB's information system, information, and missions. As a result, although the DNFSB has not achieved a level 4 calculated maturity level, the DNFSB's information security program is overall effective.

Initial Performance Summary

Department of Commerce

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	14	3	0
E-mail	330	402	423
External/Removable Media	0	0	0
Impersonation	2	6	0
Improper Usage	722	851	417
Loss or Theft of Equipment	29	38	32
Web	59	114	42
Other	284	276	274
Multiple Attack Vectors	23	33	5
Total	**1,463**	**1,723**	**1,193**

CIO Self-Assessment

The Department of Commerce (DOC) is committed to building a strong cybersecurity program that protects and enables its diverse mission. The DOC implemented a structured and systematic approach to increase cybersecurity visibility; consolidate cybersecurity structures and workflows; fill gaps in people, process, and technology while reducing enterprise-wide cybersecurity risks. The DOC Enterprise Security Operations Center (ESOC) implemented a Cyber Threat Intelligence (CTI) program to increase the collection, processing, and analysis of intelligence information from a range of sources and increased information sharing of CTI across the enterprise. Recognizing that DOC must continue to enhance its cybersecurity posture, the DOC established the Commerce Cybersecurity Task Force to address efforts to increase the adoption of cloud solutions, mature SOC capabilities, and continue efforts toward full implementation of PIV or an alternative multifactor authentication solution to better manage and protect access to the Department's data and support future deployment of a Zero Trust Architecture (ZTA).

Independent Assessment

The Department of Commerce (Department), Office of the Inspector General (OIG) completed an audit of the Department's information security program. OIG reviewed a representative subset of 15 information technology (IT) systems across the Department and its bureaus. OIG assessed each of the five functional areas (Identify, Protect, Detect, Respond, and Recover) and found Identify and Respond achieved a maturity level 3, and all other functions achieved a maturity level 2. While the Department defined policies and procedures, it did not consistently implement those policies and procedures across the selected systems. As a result, the Department's information security program has scored an overall maturity rating of level 2 (defined) and is therefore not fully effective.

Initial Performance Summary

Department of Energy

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	3	5	9
E-mail	111	103	110
External/Removable Media	1	1	3
Impersonation	0	0	8
Improper Usage	231	270	273
Loss or Theft of Equipment	157	119	179
Web	29	10	48
Other	287	215	70
Multiple Attack Vectors	1	4	0
Total	**820**	**727**	**700**

CIO Self-Assessment

The Secretary stresses cybersecurity as an agency priority and leadership across DOE play an active role in shaping cybersecurity risk management and mitigation activities. The greatest nation-state-related threats to DOE information technology (IT) and operational technology (OT) networks will likely come from nation state actors. Cybercrime groups operating on a for-profit basis represent a significant threat to Department networks as well, particularly as skilled foreign cybercriminals targeting the United States maintain relationships with these nation state actors. Successful attacks by any of these threats could result in damage, disruption, or unauthorized access to business/mission critical assets associated with the integrity and safety of personnel, nuclear weapons, energy infrastructure, and applied scientific R&D. DOE is working to combat these threats by focusing on strengthening enterprise visibility of all assets, improving situational awareness to foster near real-time risk management, improved incident response, and defense in depth. Additionally, the Department is focused on forging interagency and private sector partnerships to protect critical infrastructure; promoting information sharing, enhancing policy and guidance, and workforce/role-based training; and improving technologies for cyber defense through machine learning and big data analytics. DOE continues to leverage funding through the DHS CDM program, working to recover from funding delays caused by the COVID-19 pandemic response. As asset and vulnerability management tools are procured and deployed across DOE in the coming months we will see significant improvements in enterprise visibility and overall Information Security Continuous Monitoring and reporting.

Independent Assessment

The Office of Inspector General (OIG) conducted the annual evaluation of the Department of Energy's unclassified information security program and obtained results from the Department's Office of Enterprise Assessments related to its assessment of national security systems. Specifically, the OIG and Office of Enterprise Assessments reviewed the Department's progress towards meeting the DHS/OMB FISMA metrics for the unclassified and national security cybersecurity programs systems at 11 judgmentally selected sites. The cybersecurity programs were reviewed to assess the effectiveness of information security policies, procedures, and practices. Overall, the OIG determined that the Department was generally not effective in implementing the FISMA cybersecurity metrics at the sites reviewed. While we determined that the Department had achieved a Managed and Measurable (Level 4) maturity level for the Respond function, the remaining function areas (Identify, Detect, Protect, and Recover) were assessed at Consistently Implemented (Level 3), and we noted that improvements should continue to be made in those areas. However, due to the non-homogeneous nature of the Department's population, we noted that it is likely that the weaknesses discovered at certain sites reviewed may not be representative of the Department's enterprise as a whole, and the overall results could change from year to year depending on which locations are tested by the OIG and the Office of Enterprise Assessments.

Initial Performance Summary

Department of the Interior

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	2	1	0
E-mail	8	10	33
External/Removable Media	0	0	0
Impersonation	0	0	1
Improper Usage	255	164	35
Loss or Theft of Equipment	13	0	6
Web	17	19	75
Other	263	169	117
Multiple Attack Vectors	2	0	10
Total	**560**	**363**	**277**

CIO Self-Assessment

DOI addressed multiple IT modernization actions needed to support COVID-19 mitigation and subsequent return to work. In collaboration with DOI Bureaus and Offices, OCIO prioritized bandwidth increases for over 300 locations and accelerated network modernization previously planned to complete in September 2022, ensuring that DOI's more than 60,000 teleworking users retained secure access to the systems, applications, and data they need to execute their missions.

DOI was among many Federal agencies impacted by foreign state adversary attacks in FY21, most notably two incidents involving software vulnerabilities identified in December 2020 and April 2021 in widely used commercial products. In both cases, DOI determined that it had vulnerable software exposed during periods of adversary activity and detected early-stage signs of exploitation. DOI incident responders worked with FBI and private sector investigators as well as vendor subject matter experts to determine the extent of compromise, finding no signs of data exfiltration or persistent presence on DOI systems. In the April incident, DOI was notified by the product vendor and began mitigation and investigation activities before DHS directed agencies to take such actions. DOI has implemented enhancements to Endpoint Detection and Response (EDR) capabilities to mitigate the risk of future commercial product exploits.

DOI responded to the issuance of EO 14028 by committing to bold, transformative, and decisive actions to prioritize, modernize, and secure IT resources and assets and to focus on modernization goals that are essential to developing a Zero Trust architecture. DOI is planning enhancement efforts around identity management, data access, and network

Independent Assessment

We conducted a performance audit over the Department of the Interior's (DOI) information security program to determine the effectiveness of such program for the fiscal year (FY) ending September 30, 2021. The scope of the audit included the following 12 Bureaus and Offices: Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), Bureau of Ocean Energy Management (BOEM), Bureau of Reclamation (BOR), Bureau of Safety and Environmental Enforcement (BSEE), U.S. Fish and Wildlife Service (FWS), National Park Service (NPS), Office of Inspector General (OIG), Office of the Secretary (OS), Office of Surface Mining Reclamation and Enforcement (OSMRE), Office of the Solicitor (SOL) and U.S. Geological Survey (USGS). DOI system inventory included 160 operational unclassified information systems, and we randomly selected 12 information systems across the aforementioned Bureaus and Offices for the performance audit.

Consistent with applicable FISMA requirements, OMB policy, and NIST standards, DOI established and maintained its information security program and practices in the five Cybersecurity Functions of Identify, Protect, Detect, Respond, and Recover. The Detect Function and the Identity and Access Management and Information Security Continuous Monitoring FISMA Metric Domains were effective. However, DOI's overall information security program was not effective as we identified deficiencies in four of five Functions: Identify, Protect, Respond, and Recover. Specifically, deficiencies were noted in the associated FISMA Metric Domains of Risk Management, Configuration Management, Data Protection and Privacy, Security Training, Incident Response, and Contingency Planning.

We assessed the Detect Function as Managed and Measurable (Level 4) and the Identify, Protect, Respond and Recover Functions at Consistently Implemented (Level 3). Overall, we modernization to supplement ongoing activities to securely transition to cloud, expand the use of multifactor authentication, and ensure encryption of data at rest and in transit.

assessed DOI’s information security program and practices as Consistently Implemented (Level 3) and ineffective.

Initial Performance Summary

Department of Justice

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	2	0
E-mail	378	246	200
External/Removable Media	1	0	0
Impersonation	0	0	0
Improper Usage	199	114	90
Loss or Theft of Equipment	14	3	3
Web	9	2	1
Other	184	81	113
Multiple Attack Vectors	1	2	0
Total	**787**	**450**	**407**

CIO Self-Assessment

The Office of the Chief Information Officer has continued to emphasize the importance of multi-factor authentication (MFA) and has made significant strides in the issuance of PIV within the Department. Over the course of the last fiscal year the Department has achieved 97% issuance, which is a critical step towards meeting full adoption of MFA. In the wake of the SolarWinds breach, the Department has formulated the design and build of Zero Trust capabilities, which are being implemented into the enterprise security architecture, standard security practices, and policies, to combat the evolving sophistication of our adversaries and supply chain risks. These capabilities address weak vendor configurations and provide better security controls to improve the Department's posture. The OMB also designated DOJ as a federal shared service provider for Security Operations Center (SOC) services, supporting government-wide initiatives to consolidate and share services whenever possible.

Independent Assessment

During fiscal year 2021, the Department of Justice (Department) Office of the Inspector General (OIG) reviewed the information security programs of 6 Department components and a sample of 14 systems within these components. As a result of our review, the OIG determined that the maturity level for the Department's information security program is "Level 3 - Consistently Implemented" across three Security Functions: Identify, Detect, and Recover; and "Level 4 - Managed and Measurable" for the Security Functions of Protect and Respond. Therefore, the OIG determined that two of the five Security Functions: Protect and Respond, are effective. However, the OIG determined that the Department's overall information security program is not effective due to the exceptions noted within the three Security Function areas of Identify, Detect, and Recover. The Department should implement our recommendations specifically within the Risk Management, Supply Chain Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Security Training, Information Security Continuous Monitoring, Incident Response, and Contingency Planning metrics of the Identify, Protect, Detect, Respond, and Recover Functions to improve the effectiveness of the Department's information security program.

Initial Performance Summary

Department of Labor

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	1	7
E-mail	25	17	30
External/Removable Media	1	0	0
Impersonation	0	0	0
Improper Usage	96	111	190
Loss or Theft of Equipment	97	80	59
Web	2	5	4
Other	100	109	105
Multiple Attack Vectors	0	2	1
Total	**322**	**325**	**396**

CIO Self-Assessment

In Fiscal Year 2021, DOL took significant steps to enhance the effectiveness of its cybersecurity program, including for areas prioritized under Executive Order (EO) 14028, Improving the Nation’s Cybersecurity. DOL developed a roadmap for Zero Trust, enhanced policy and procedure for Secure Supply Chain, and continued implementing enterprise-wide solutions to enhance encryption, multifactor authentication, IT asset management, incident response and monitoring. In particular, DOL continued deployment of additional DHS Continuous Diagnostics and Mitigation tools for vulnerability management, implementation of new Data Loss Prevention mechanisms, and transition of FISMA systems due for periodic reauthorization into Ongoing Authorization. DOL provided additional risk-based security and privacy awareness trainings, including quarterly phishing exercises, to address increased cybersecurity risks faced by remote users. Across these areas, DOL maintained its focus on capability effectiveness, meeting targets across all Cybersecurity Cross Agency Priorities.

In the area of incident detection and response, DOL continues to collaborate with DHS to take a more automated approach to incident response, and successfully deployed new capabilities as part of the Vulnerability Disclosure Program, enhancing its 24x7 Security Operations Center (SOC) to substantially reduce critical vulnerabilities within DOL.

DOL will continue to focus on strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. DOL intends to: continue to improve in the adoption of MFA and encryption of data-at-rest and in-transit; reinforce and improve in the protection of critical software and mature capabilities for supply chain risk management;

Independent Assessment

We identified 43 issues that were consolidated into 15 findings for the FY 2021 performance audit report. The nature of these findings affected our overall assessment of the Cybersecurity Functions. To improve its information security program, DOL should design, implement, and monitor qualitative and quantitative key performance indicators to measure the effectiveness of its Identify, Detect, and Recover processes and activities. DOL should also enhance its key performance indicators for Configuration Management and Identity and Access Management. Additionally, DOL should develop and implement Plans of Action and Milestones (POA&Ms) to remediate the 15 FY 2021 audit findings.

Additionally, we assessed the overall DOL IT security program as not effective based on the mode of the individually assessed maturity levels for the 66 metrics, as directed by the FY 2021 IG FISMA Reporting Metrics guidance. Specifically, the Protect and Respond Cybersecurity Functions were assessed as Managed and Measurable (Level 4), while the Identify, Detect, and Recover Cybersecurity Functions were assessed as Consistently Implemented (Level 3).

For the FY 2021 performance audit, our scope included assessing the maturity levels for the FY 2021 IG FISMA Reporting Metrics and testing the NIST 800-53 security controls referenced in these metrics at the entity level, for 15 selected DOL operated information systems, and for 5 selected contractor information systems. In addition, we followed up on the status of 43 prior-year FISMA recommendations.

continue efforts to transition DOL's network infrastructure to IPv6; and, continue SOC enhancements that will allow DOL to anticipate and mitigate risk, and stay ahead of the evolving threat landscape.

Initial Performance Summary

Department of Transportation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	2	3	2
E-mail	15	6	13
External/Removable Media	1	3	0
Impersonation	0	1	1
Improper Usage	92	85	67
Loss or Theft of Equipment	0	1	3
Web	40	25	26
Other	157	130	248
Multiple Attack Vectors	4	5	2
Total	**311**	**259**	**362**

CIO Self-Assessment

The Department of Transportation identified multiple risks to the agency during FY 2021:

- The agency assessed that its current practices and prioritization of resources were not effectively addressing a backlog of audit recommendations. In response, the agency's new CIO directed a review of all open audit recommendations, and identification of accountable components and officials who will be required to ensure that they act upon recommendations within their purview.

- The agency identified that its logging infrastructure was insufficient to support detection and analysis by the agency enterprise SOC. In response, the agency accelerated plans and reprioritized resources to acquire and develop an enterprise logging capability that is elastic, and scalable.

- The Department of Transportation had vacancies in two key positions during FY 2021, the Chief Information Security Officer, and the Chief Privacy Officer. The agency's new CIO has acted with IT senior leadership, the CFO and HR staff, to gain support for accelerating the search for and recruiting of candidates for these positions.

- The agency determined that there were multiple gaps in coverage and capabilities across the agency enterprise networks that potentially limited visibility, failed to identify and mitigate threats, and limited the agency's ability to manage and protect agency assets. In response, the agency accelerated pre-existing plans for EDR, IT management, and cloud security features.

- Lastly, the agency identified a retreat from a previous high-level of compliance with mandatory PIV/MFA usage on

Independent Assessment

Based upon our audit of DOT's information security program, we concluded that DOT is at the Defined maturity level - the second lowest level in the maturity model for an information security program, and thus not effective. Specifically, four functional areas achieved a maturity level of Defined (Level 2) with one functional area achieving a Consistently Implemented (Level 3) maturity level for an overall maturity level of Defined for the security program. There are longstanding security deficiencies similar in type and risk level to prior years and an overall inconsistent implementation of the security program. Specifically, we noted weaknesses in eight of the nine IG FISMA Metric Domains such as risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction. Many of these weaknesses can be attributed to an inconsistent enforcement of an agency-wide information security program across the enterprise, ineffective communication between the Operating Administrations, the lack of progress in the remediation of prior year audit recommendations, not having a multi-year strategy and approach for addressing long standing FISMA weaknesses, and not having a permanent Chief Information Security Officer (CISO) and Chief Information Officer (CIO), which detracts from the leadership, oversight, and accountability needed to address ongoing information security program weaknesses.

agency networks. In response, the CIO has declared a 60-day Cyber Sprint, with mandatory PIV/MFA as a priority, followed by acquisition and deployment of an alternative MFA solution to support strong authentication requirements.

Initial Performance Summary

Election Assistance Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

The Commission continues to operate in a 100% Work from Home environment. All users are required to utilize provided VPN to connect to Commission resources. Phishing continues to be a major threat with one spearfishing attempt in the past FY. The Phish was identified early and no breach occurred. Phishing tests are conducted monthly with remediation training available to all. Cybersecurity Awareness training on current topics is continuously available via on demand streaming. Specific cybersecurity staff training and and hiring have also been accomplished during the past year.

Independent Assessment

We assessed the EAC’s security control effectiveness and the extent to which the controls were implemented correctly, operating as intended, and meeting the security requirements for the information system. EAC OIT generally had policies for its information security program and has consistently implemented security controls.

Initial Performance Summary

Department of Education

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	1	1
E-mail	0	1	1
External/Removable Media	0	0	0
Impersonation	0	1	0
Improper Usage	62	51	44
Loss or Theft of Equipment	0	0	1
Web	0	5	1
Other	17	0	45
Multiple Attack Vectors	0	0	1
Total	**79**	**59**	**94**

CIO Self-Assessment

During FY 2021, the Department successfully maintained information technology (IT) services to support 100 percent telework in response to the COVID-19 pandemic without impact or compromise to the Department's cybersecurity or privacy risk posture. Education continued regular communications to Department users to emphasize cyber vigilance and individual responsibilities for data protection and privacy. Education also simulated phishing exercises around the current threat landscape to keep Department employees current and educated. As a result of these efforts, the Department has been able to continue its important mission of nationally delivering regular and additional pandemic funding for educational programs without interruption.
Information and IT resources are critical to the Department's ability to provide quality services and support education across our great Nation. Throughout this year, the Department implemented tools, processes, and protections to maximize the quality, security, and privacy of our information systems. It also continued to develop and implement uniform and consistent governance policies and standards to strengthen the Department's cybersecurity by enhancing the confidentiality, integrity, and availability of its information technology infrastructure, systems, and data. Based on the FY 2021 CIO FISMA metrics, the Department is effectively managing risk.

Independent Assessment

Our objective was to determine whether the U.S. Department of Education's (Department) overall information technology (IT) security programs and practices were effective as they relate to Federal information security requirements. To answer this objective, we rated the Department's performance in accordance with FY 2021 Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics. We determined the Department's programs were consistent with Level 2–Defined, which is considered not effective for three domains: Supply Chain Risk Management, Identity and Access Management, and Data Privacy and Protection, and Level 3–Consistently Implemented, which is considered not effective for six domains: Risk Management, Configuration Management, Security Training, Information System Continuous Monitoring, Incident Response, and Contingency Planning.

Initial Performance Summary

Equal Employment Opportunity Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	1	4
Multiple Attack Vectors	0	0	0
Total	**1**	**1**	**5**

CIO Self-Assessment

In FY 2021, the EEOC continued modernizing its technology infrastructure, including significant development of its TMF-funded HVA system, and mitigating major risks. As in FY 2020, the pandemic presented significant operational challenges to extend remote work capabilities in a safe, robust, and secure manner. To continue to meet these challenges, the agency completed an enterprise operating system upgrade, upgraded and further secured its virtual private network solution, enabled multi-factor authentication, and implemented a secure share solution to better protect sensitive and confidential data. Additional efforts, focused on the agency's infrastructure, included decommissioning the agency's legacy website and Intranet platform; deploying a Hardware Security Module to provide enterprise PKI certificates for workstations, servers, and applications; utilizing virtual desktop technology to support its intern program; and continuing to expand the agency's cloud presence. The EEOC also increased enterprise cybersecurity visibility and resilience, and significantly improved logging, event monitoring, and incident handling in its cloud tenant. Last, the EEOC improved its security posture through compliance with government cybersecurity requirements, including Binding Operational Directives (BoD) 20-01 and 18-01; critical threats in Emergency Cyber Directives (ED) 21-01, 21-02, 21-03, and 21-04; and FISMA and DHS' Cyber-Hygiene programs. As staff have not been in the office for 20 months, full deployment of PIV multi-factor authentication now is expected to be substantially completed 150 days after the Agency begins reentry from full-time telework.

Independent Assessment

EEOC has an overall effective information security program. EEOC has can further strengthen its information security program by fulling implementing planned actions in FY 22.

Initial Performance Summary

Environmental Protection Agency

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	2	11	15
External/Removable Media	0	0	1
Impersonation	0	0	0
Improper Usage	102	15	1
Loss or Theft of Equipment	33	37	40
Web	0	8	22
Other	63	36	16
Multiple Attack Vectors	1	3	0
Total	**201**	**110**	**95**

CIO Self-Assessment

EPA has maintained an overall rating of “Managing Risk” on the FY 2021 Risk Management Assessment. The evolving Cybersecurity landscape and the increasing sophistication of malicious threat actors require we stay vigilant and continue strengthening our cyber defenses and risk management processes. The expansion of telework to meet mission needs during the ongoing COVID-19 pandemic has created remote access management risks that we continue to address, such as privileged network access management with our ongoing transition to EPA’s Privileged Access Management (PAM) solution and the implementation of alternative multi-factor authentication mechanisms for privileged and non-privileged users. To address risks associated with unauthorized access, data encryption and data exfiltration, EPA implemented a Data Loss Prevention (DLP) capability for email encryption and to prevent the usage of untrusted removable media. While still in monitoring mode, enforcement of DLP policies will be implemented by the end of this year. EPA will continue working towards full DLP deployment across on the Enterprise network. In FY 2021, EPA invested significant resources to fully transition Continuous Monitoring (CM) tools to O&M, providing greater visibility across the Enterprise operational environment and resulting in a 92% decrease in the timely remediation of identified vulnerabilities. Additionally, the EPA has implemented an Enterprise Endpoint Detection and Response solution enabling near real-time identification, analysis, and remediation of Cybersecurity incidents and proactive prioritization of cyber threat response activities. In FY 2022 and beyond, the EPA will continue focused efforts to achieve the overall objective of the federal cyber security requirements, including the EO, to defend against cyber threats and risks and safeguard our assets.

Independent Assessment

EPA has demonstrated it has consistently implemented policy, procedures, and strategies for all five of its information security function areas. The Office of Inspector General assessed the five Cybersecurity Framework function areas and concluded that EPA has achieved a Level 3, Consistently Implemented, which denotes that the Agency has consistently implemented policies, procedures, and strategies in adherence to the Fiscal Year 2021 Inspector General Federal Information Security Modernization Act reporting metrics. While EPA has policies, procedures, and strategies for these function areas and domains, improvements are still needed in the following areas:

(1) Risk Management – EPA’s software management process lacks documented procedures for detecting and removing unapproved software on the EPA network resulting in unapproved software installed on its region and program office networks.

(2) Configuration Management - EPA has not updated its Risk Assessment or Systems and Information Integrity procedures to meet the Department of Homeland Security Binding Operational Directive 19-12, Vulnerability Remediation Requirements for Internet-Accessible Systems, a federal requirement for remediating critical vulnerabilities within 15 calendar days of initial detection.

Initial Performance Summary

Export-Import Bank of the United States

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**1**

CIO Self-Assessment

The Export-Import Bank of the United States (EXIM) continues to build on a strong and robust cybersecurity program. This year, EXIM has focused on three (3) key areas that address our need to maintain information security amidst the new COVID reality and meeting new Supply Chain Risk Management mandates from the Executive Branch. First is our ongoing effort to provide secure and private remote access to mission critical systems during the COVID pandemic. Next, EXIM is diligently responding to mandates for Executive Order 14028 on Improving the Nation's Cybersecurity. Finally, EXIM is planning for its workforce re-entry. During the COVID-19 pandemic, EXIM increased opportunities for remote work and implemented several steps to mitigate potential incidents, threats, and attack vectors that have arisen. In planning for the workforce re-entry, EXIM is actively implementing technologies, such as desktop virtualization, that creates flexibility to meet the requirements of new work arrangements while simultaneously improving its ability to effectively and efficiently manage the IT security of a distributed workforce. EXIM also mitigates cybersecurity risks to the agency from a holistic standpoint, which includes improved vulnerability management and internal auditing processes, and the enhancement of our Information Security Continuous Monitoring (ISCM) program through our partnership with the DHS Shared Services and Continuous Diagnostics and Mitigation (CDM) programs. EXIM also strengthened its incident response posture by conducting multiple training exercises to mitigate risk associated with telework and bank operations. EXIM has also enhanced its security awareness and phishing training by highlighting telework-specific risks. EXIM recognizes the advanced threats facing its environment and will continue to examine ways to improve its internal processes and practices and cybersecurity awareness

Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, EXIM has established and maintained its information security program and practices for the five Cybersecurity Functions and eight FISMA program areas. Although we noted deficiencies impacting specific questions within the RM, IAM, ST, and CP metric domains, we determined its information security program was effective as we evaluated the majority of the FY 2021 IG FISMA Reporting Metrics at the Managed and Measurable (Level 4) or higher maturity levels.

outreach efforts to stakeholders.

Initial Performance Summary

Farm Credit Administration

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	4	1
Loss or Theft of Equipment	15	3	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**15**	**7**	**1**

CIO Self-Assessment

The Farm Credit Administration continues to leverage its information technology (IT), risk-management program to improve the agency's risk posture. We rigorously manage our risks under NIST guidance, a next-generation risk model and a process to maximize the agency's limited resources. Following this process over the past year, with weekly briefings, and focused project efforts, we have mitigated or closed nearly 20% of our known risks.

FCA continued to improve multi-factor authentication, increased our use of cloud services, improved data integrity protection capabilities, implemented device-level access control, and improved mobile device management. In addition, we enforce VPN connection from all our laptop computers, thereby reducing the agency's risk surface area.

FCA also improved our security and privacy maturity by publishing key documents to include: a Common Controls Catalog, an information security policy, Personally Identifiable Information Collection and Use guidance, Incident Management and Breach Response procedures, Controlled Unclassified Information plan, and an IT Contingency Plan.

To ensure the security of examination data, FCA conducts intrusion prevention, encrypts sensitive database content, and ensures TLS-encrypted connections with 100% of our institutions. FCA also manages our mobile devices, we restrict use based on policy and wipe lost devices.

Independent Assessment

The Office of Inspector General contracted with an independent audit firm to conduct an audit on the Farm Credit Administration's (FCA) information security program. FCA's information security program is guided by a robust, entity-wide risk management program. Critical functions, such as Identify and Detect, were rated at the level of Managed and Measurable. Based on the metrics utilized to determine the effectiveness of the information security program, the audit firm determined that FCA had an effective information security program with an overall rating of Level 4: Managed and Measurable.

FCA's information security environment included the following key elements:

- information security policies and procedures,
- risk-based approach to information security,
- risk management tools,
- risk management automated tracking,
- implementation of risk-based security controls,
- corrective action for significant information security weaknesses,
- Change Control Board,
- user agreements and personal risk designations,
- standard baseline configurations,
- patch management process,
- vulnerability and security control assessments,
- alerts for suspicious activity and devices,
- security training program,
- continuous monitoring, and
- weekly security meetings.

The audit firm identified opportunities for FCA to continue to improve the program and made three recommendations.

Initial Performance Summary

Federal Communications Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	1	1
E-mail	4	1	7
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	14	22
Loss or Theft of Equipment	8	5	0
Web	20	5	2
Other	12	61	46
Multiple Attack Vectors	0	0	1
Total	**45**	**87**	**79**

CIO Self-Assessment

The FCC recognizes the following cybersecurity risks to the agency:
1. Security ATOs not completed for all organization operated systems.
2. Findings and Recommendations from IG's FY 2020 FISMA Evaluation.
3. "Critical" and "High" vulnerabilities not remediated within their stated timelines.
4. Lack of full PIV implementation for user authentication.
5. Disaster recovery / continuity planning due to COVID-19 mandatory telework.
6. Portable media drives, hard drives, USBs are not able to be scanned for malicious files during mandatory telework.

The FCC has taken the following steps to mitigate these risks:
1. FCC has developed a 3 year plan to get to 100% ATOs by the end of 2023.
2. FCC has developed and implemented corrective action plans for all findings from IG's FY 2020 FISMA Evaluation.
3. FCC has developed a plan to remediated "Critical" and "High" vulnerabilities by September 2022.
4. FCC is currently implementing identified solutions for multi-factor authentication.
5. Migrated the Virtual Desktop Infrastructure to Microsoft Azure Cloud.

Independent Assessment

The fiscal year (FY) 2021 FISMA evaluation included the Federal Communications Commission's (FCC) network (i.e., FCCNet), the FCC's core financial management system (i.e., Genesis), and the FCC's report filing system for telecommunication service disruptions pursuant to FCC rules (i.e., Network Outage Reporting System [NORS]). Kearney & Company, P.C. (Kearney) assessed the FCC's security processes related to the five National Institute of Standards and Technology (NIST) Cybersecurity Functions and determined that three functions (Detect, Respond, and Recover) were at a maturity Level 4, Managed and Measurable and two functions (Identify and Protect) were at a maturity Level 3, Consistently Implemented. Due to the removal of one of the Detect Function FISMA metric questions between FY 2020 and FY 2021, the FCC's Detect Function maturity level calculation increased to a Level 4, Managed and Measurable in FY 2021 from a Level 2, Defined in FY 2020. Going forward, we recommend that the FCC implement its documented security policies and procedures and establish ongoing monitoring over all five NIST Cybersecurity Functions to achieve an effective maturity Level 4, Managed and Measurable, for its Information Security Program. Kearney and the FCC Office of Inspector General (OIG) determined that the FCC's overall program was effective in FY 2021.

Initial Performance Summary

Federal Deposit Insurance Corporation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	3	0
External/Removable Media	1	1	0
Impersonation	0	0	0
Improper Usage	77	56	75
Loss or Theft of Equipment	0	0	0
Web	0	3	0
Other	2	0	5
Multiple Attack Vectors	0	0	0
Total	**80**	**63**	**80**

CIO Self-Assessment

The FDIC continues to prioritize and enhance its cybersecurity program to mitigate risks and emerging threats. Given the FDIC's mission as a financial regulator, cybersecurity risks to the FDIC are similar to those faced by other federal organizations and the financial industry at large. The risks to the FDIC span the cybersecurity spectrum to include: sophisticated and financially motivated threat actors, a complex mix of commercial and legacy assets, enterprise security architecture, and governance. The FDIC continues to prioritize and enhance its cybersecurity program to mitigate risks and emerging threats. Despite the challenges brought by the pandemic, the FDIC continues to fulfill its core mission of maintaining stability and public confidence in the nation's financial system. Actions taken in FY 2021 include further development of key policies and procedures impacting essential security control areas (e.g., release of its first corporate-wide Supply Chain Risk Management Program directive, defining related policy, roles, and responsibilities. FDIC also issued a System Security Authorization Process Guide to support the continuous monitoring of its information systems and assist FDIC stakeholders responsible for ensuring or managing information system security and privacy). Key Area of focus in 2021 has been integrating the Risk Management Framework (RMF) into business processes, contracts and projects and embedding RMF into CIOO lifecycle planning and governance as those functions take shape. There is also a multi-year Document Labeling initiative to effectively Identify, Categorize, Label, and Protect FDIC information and data, minimizing the risk associated with data leakage, improve information security and data management practices, and facilitate appropriate information sharing.

Independent Assessment

The FDIC's information security program was operating at a Maturity Level 4 (Managed and Measurable). The audit covered key components of the FDIC's information security program and selected controls pertaining to two general support systems, one major application, and one contractor service. During the past year, the FDIC had established certain information security program controls and practices. In addition, the FDIC worked to strengthen its security controls following the issuance of our FISMA 2020 audit report. Specifically, the FDIC updated its Privacy Program; created processes to prevent unauthorized software from being installed on the FDIC network;reviewed Risk Acceptance decisions;defined and implemented the oversight authorities, roles, and responsibilities of its Operating Committee;enhanced procedures for employee and contractor investigations;updated contingency planning policies and procedures;and conducted tests of the contingency plan. However, the audit report describes significant security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices and that can be improved to reduce the impact to the confidentiality, integrity, and availability of the FDIC's information systems and risk to data. The highest risk weaknesses involved the need for FDIC to: ensure POA&Ms are addressed timely;define processes and procedures that support the underlying components of its SCRM directive;strengthen controls for Administrative Accounts;and ensure all of its systems are subjected to a proper risk assessment, authorization to operate, or ongoing monitoring in accordance with the RMF. The audit resulted in six recommendations intended to improve the effectiveness of FDIC's security program and practices. The FDIC concurred with all six recommendations and planned to complete corrective actions by December 2022. The FDIC was also working to address an additional six recommendations from prior FISMA audit reports.

Initial Performance Summary

Federal Energy Regulatory Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	0	1	0
Other	0	0	97
Multiple Attack Vectors	0	0	0
Total	**0**	**1**	**98**

CIO Self-Assessment

In FY 2021, FERC continued to make significant investment in maintaining, evolving and maturing our risk-based, cost effective cybersecurity program. Some highlights include: 1) Enhanced our Data Loss Prevention (DLP) solution and Controlled Unclassified Information (CUI) protections to limit USB/DVD/CD capabilities and updated monitoring and reporting; 2) Deployed Privileged Access Management (PAM) and updated elevated account process to ensure secure administration of IT tools and provide improved audit capabilities for all administrator work; 3) Created/updated secure baselines for 29 new and existing technologies; 4) Created secure governance policies and processes around Office 365 online tools. While cybersecurity risks constantly evolve, the COVID-19 national emergency presented its own risks to productivity, continuity, and securely conducting business. FERC has been committed to ensuring a secure remote work environment through additional user guidance and training, procuring products to increase bandwidth and user experience, and maintaining transparency and availability to all users as needs arise or change.

Independent Assessment

The OIG conducted its annual evaluation of FERC's unclassified information security program to assess the effectiveness of its related policies, procedures, and practices within five information security functions (Identify, Protect, Detect, Respond, and Recover). The OIG determined that FERC had an effective information security control environment. Specifically, FERC was rated “Managed and Measurable” (Level 4) in the Identify, Protect, Detect, and Respond functions, and "Consistently Implemented" (Level 3) in the Recover function.

Initial Performance Summary

Federal Housing Finance Agency

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	0
Loss or Theft of Equipment	13	5	1
Web	0	0	0
Other	1	2	5
Multiple Attack Vectors	0	2	0
Total	**15**	**9**	**6**

CIO Self-Assessment

FHFA continued to demonstrate an effective information security program in FY21 while planning for and implementing new requirements set forth in NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and organizations, as well as Executive Order (E.O.) 14028, Improving the Nation's Cybersecurity, and subsequent guidance resulting from the E.O. Consistent with FHFA's approach in FY20, FHFA authorized the use of non-PIV authentication for new users who could not be issued HSPD-12 cards due to the closure of FHFA's headquarters. FHFA's alternative multi-factor authentication solution is impersonation-resistant and meets NIST SP 800-63-3 AAL 2 requirements. In FY21 FHFA changed its system characterization methodology and re-characterized a number of operational cloud-based systems as FISMA Reportable. While a number of these systems are FedRAMP authorized, FHFA has not yet issued Agency ATOs for these systems, which is planned to be completed by FY22 Q2.

The FHFA independent public accounting firm contracted by the FHFA Office of Inspector General (OIG) to audit the effectiveness of FHFA's information Security Program concluded that "FHFA implemented an effective information security program and practices and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall Managed and Measurable maturity level."

Independent Assessment

An independent public accounting firm (IPA) under contract and supervision of the Federal Housing Finance Agency (FHFA) Office of Inspector General completed a performance audit to evaluate the effectiveness of FHFA's Information Security Program and practices and respond to the Department of Homeland Security's FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics, dated May 12, 2021 (FY 2021 IG FISMA Reporting Metrics). The IPA's methodology included testing the effectiveness of selected security controls implemented in a subset of systems in accordance with the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and Organizations. The IPA determined that FHFA implemented an effective information security program and practices and complied with FISMA and related information security policies and procedures, standards, and guidelines by achieving an overall Managed and Measurable maturity level. Although FHFA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, the IPA noted weaknesses in four of the nine domains in the FY 2021 IG FISMA Reporting Metrics. As a result, the IPA made three recommendations to assist FHFA in strengthening its information security program.

Initial Performance Summary

Federal Labor Relations Authority

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**0**

CIO Self-Assessment

The Federal Labor Relations Authority, like all government agencies, is a constant target. This year's FISMA assessment included an array of controls testing. The controls selected were from NIST 800-53 and mapped to the CyberScope questions. The agency has made numerous strides this year, as a large number of prior year findings were closed in the current year. The agency conducted extensive cyber security training for users as well as additional training for the information technology staff. The agency continues to explore other way to make it's systems more secure, from multifactor authentication to ensuring all systems encrypt data at rest.

Independent Assessment

This year's FISMA assessment included an array of controls testing. The controls selected were from NIST 800-53 (Rev. 4 and 5) and mapped to the Cyberscope questions. The agency (FLRA) has made numerous strides this year, as a large number of prior year findings were closed in the current year. Although the FLRA is a small agency as compared to the larger agencies (e.g. CFO Act agencies), and has a small IT staff; the agency is quite effective in deploying IT controls throughout the agency.

Initial Performance Summary

Federal Maritime Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	4	4
Multiple Attack Vectors	0	0	1
Total	**0**	**4**	**5**

CIO Self-Assessment

The FMC has performed bi-annual risk assessments as defined by NIST to identify, estimate, and prioritize cybersecurity risk to the agency operations, assets, staff, and the public. We have identified the agency's critical information systems assets and determined the impact on the agency in the event of a cyber-attack or security incident. To protect the Commission's information technology assets, the agency has deployed security standards in response to DHS' Binding Operations Directives and continues to reduce internal and external vulnerabilities through the implementation of the Continuous Diagnostics and Mitigation (CDM) program cybersecurity tools and services and through implementing MTIPS.

Independent Assessment

The overall Inspector General (IG) assessment rating is "effective" for the Federal Maritime Commission's (FMC) information security program for fiscal year (FY) 2021. In the IG's FY 2021 FISMA audit, the OIG identified one new audit finding, closed one prior year audit recommendation, and noted the agency’s progress on another outstanding prior year recommendation.

Initial Performance Summary

Federal Mediation and Conciliation Service

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	4	3
Multiple Attack Vectors	0	0	0
Total	**2**	**4**	**3**

CIO Self-Assessment

We have followed our cyber-security framework action plan and have several contractors who have performed cyber-security assessments. The results of these assessments included an implementation plan to re-mediate identified risks and provide a mechanism for continued evaluation. Our Managed Security Services Provider (MSSP) continues monitoring in FY 2021. We have modified our SSP to align with NIST 800-53 moderate and are working on maturing implementation statements. FMCS had significantly mitigated telework risk prior to 2020. CISA performed internal and external penetration tests FY 2021 and we are remediating the results. By performing these actions, we believe we have made significant progress towards achieving level 4 maturity for these metrics.

Independent Assessment

Our overall agency wide information security program is robust and effective based on the risk posture that we have accepted. We have many protective measures and policies in place and are handling threats adequately while slowly improving in all areas. Our greatest challenge is balancing the time required to gain the proper level of expertise to manage any newly implemented technologies while keeping up with the daily maintenance and support with a small staff. There are only so many hours in a day and all the money in the world does not change that. This is just the reality of being small. We continue to make progress towards full implementation of some measures that are currently underway in coordination with our cyber-security framework action plan. We are utilizing several contractors to perform services that we simply do not have the expertise nor the time to perform. We continue to expand the capabilities of our automated monitoring tools and have had several comprehensive cyber-security assessments conducted that have produced POA&Ms to successfully re-mediate any deficiencies identified. We will continue to replace or improve any deficient processes where possible in FY 2022 and beyond. By performing these actions, we believe we will make significant progress towards achieving level 4 maturity for these metrics.

Initial Performance Summary

Federal Mine Safety and Health Review Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	
Protect	Managing Risk	
Detect	Managing Risk	
Respond	Managing Risk	
Recover		
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	2
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**2**

CIO Self-Assessment

The Federal Mine Safety and Health Review Commission (FMSHRC) remains vigilant of the potential vulnerabilities identified by CISA. FMSHRC has migrating our network to the another mail platform in addition to using cloud solutions to mitigate risk.

FMSHRC will continue to monitor daily activities on our network and continue to apply applicable patches as they are released while working with our ISP to mitigate vulnerabilities.

MX Update
o This changed inbound mail to reach Exchange Online Protection (EOP) first, then cross the hybrid connection for mail destined for mailboxes still hosted on prem. This made the EOP servers begin scanning all inbound mail for SPAM\Virus
Outbound Mail SEND modification
o This changed outbound mail to go through EOP servers on the way out. This was done to have outbound mail show as coming from O365 instead of our on prem IP that had been blacklisted, but also provides additional benefits of allowing EOP servers to scan our outbound mail for SPAM\Virus
Implement DMARC and DKIM
o This was done so that our outbound mail passes both DMARC and DKIM checks being done at the mail environment receiving the mail
Inbound Whitelist Transition
o This moved the inbound safe senders configuration from the “Allowed Domains” listing on the SPAM Policy to a Transport rule. This was done to increase security of inbound mail by preventing mail domain spoofing of inbound domains that we trust.

Independent Assessment

Initial Performance Summary

Board of Governors of the Federal Reserve

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	1	1
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	1	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	5	8
Multiple Attack Vectors	0	0	0
Total	**3**	**7**	**9**

CIO Self-Assessment

For 2021, the primary cybersecurity risks to the Federal Reserve Board (FRB) included the continued 100% remote work posture due to the pandemic; phishing emails carrying advanced malware; ransomware; and distributed denial-of-service (DDOS) attacks that target the availability of data and systems; vendor risks, such as the supply chain compromise from Dec 2020 that impacted the Federal Government at large and an increase in the usage of cloud service providers at the Board; and trusted insiders with access to sensitive data. Prior to 2021, the FRB had already deployed a layered approach to addressing these risks: Layered perimeter security that includes, web content filtering, intrusion prevention, email filtering, Einstein 3A monitoring services, and Data Loss Protection (DLP); next generation endpoint and network based security; enforcement of two-factor authentication for all users (privileged and non-privileged); enhanced monitoring of user behavior; encryption of all sensitive application data at rest ; anti-DDOS protections; high availability configurations of critical systems and services; conducting network monitoring for anomalies and suspicious activity; conducting end-user security awareness training to include phishing awareness simulations to ensure that users are aware of real-world phishing attack methods and the risks associated with these attacks; red and purple team tests; and multiple third party assessments beyond the work done by the Office of Inspector General. During 2021, the FRB continued to enhance its cyber security posture. Key efforts in this space included a refresh of the FRB ICAM strategy and creation of a dedicated ICAM unit; accelerating plans to enhance the use of Multifactor within the organization; continuous enhancement of our logging and monitoring capabilities, specifically in the cloud space; continuous enhancement of secure collaboration to support

Independent Assessment

Overall, we found that the Board continues to maintain an effective information security program. In addition, the Board has taken actions to address 8 of 15 recommendations that were open from our previous FISMA reviews. However, we identified opportunities to strengthen the Board's information security program across all five Cybersecurity Framework security functions–identify, protect, detect, respond, and recover–to ensure that its program remains effective. Our 2021 report includes 2 new recommendations to strengthen the Board's cybersecurity risk management processes related to plans of actions and milestones and risk acceptances.

both full remote and hybrid work environments; addressing the Cyber EO.

Initial Performance Summary

Federal Retirement Thrift Investment Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	4	11	2
Loss or Theft of Equipment	13	3	15
Web	0	0	0
Other	5	6	49
Multiple Attack Vectors	0	0	0
Total	**22**	**20**	**66**

CIO Self-Assessment

In FY 2021, the Federal Retirement Thrift Investment Board (FRTIB, or "the Agency") upheld its Federal Information Security Management Act (FISMA) maturity. FRTIB was independently evaluated for FISMA maturity and was assessed as being "Managed and Measurable" (or Level 4) in seven of the eight scoreable FISMA domains. Based on the maturity ratings across nine (9) FISMA domains, the independent auditor concluded that FRTIB had an effective information security program in FY 2021. The Agency continues to take the security program and FISMA maturity extremely seriously; during FY 2021, it expanded existing efforts to improve its information security posture and maturity on several fronts through the further definition and implementation of processes across security domains. It has also further defined metrics to assess the effectiveness of the program. In addition, the Agency has made further progress on the implementation of the government-wide Cross Agency Priority (CAP) goals. Of the ten CAP goals for FY 2021, the agency has achieved all but one, specifically: Software Asset Management – the Agency rolled out its implementation of Application Whitelisting. The full enterprise execution encountered some delays as there were issues for enterprise software applications that resulted in unacceptable impacts to business operations. The Agency is focused on solutions that permit enterprise coverage within a Zero Trust model without blocking legitimate, necessary applications as part of its transition to managed services. Maturity in FISMA compliance and achievement of CAP goals will always remain a top priority for the Agency, and focused efforts similar to the above will continue in FY 2022 (and beyond), with a goal of further strengthening the Agency's maturity across all FISMA domains.

Independent Assessment

Williams Adley determined that the Federal Retirement Thrift Investment Board (FRTIB) has maintained a mature information security governance structure and implementation of the risk management framework resulting in an "effective" organization-wide information security program in FY 2021. To determine the effectiveness of FRTIB's information security program and practices in FY 2021, Williams Adley selected a representative subset of FRTIB's information systems to assess.

For the FY 2021 reporting period, FRTIB achieved a Managed and Measurable (Level 4) maturity rating in seven (7) of nine (9) FISMA domains, a Defined (Level 2) maturity rating in one (1) of nine (9) FISMA domains, and an Ad-Hoc (Level 1) maturity rating in one (1) of nine (9) FISMA domains. Furthermore, the FRTIB was able to successfully close four (4) prior year recommendations and Williams Adley issued four (4) recommendations to address any conditions identified and their associated root causes.

Initial Performance Summary

Federal Trade Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	1	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	7	17	17
Loss or Theft of Equipment	2	1	0
Web	0	0	0
Other	0	0	22
Multiple Attack Vectors	0	0	0
Total	**10**	**19**	**39**

CIO Self-Assessment

The Federal Trade Commission (FTC) continues to manage Essential Supporting Activities (ESA) by taking a risk-based, mission-effective, cost-efficient approach. For example, when feasible the Agency uses DHS CISA services such as web application scanning. We are currently examining how to partner with DHS on implementing CDM, phishing campaign assessment (PCA) and implement DHS TIC 3.0 compliant services with DHS CLAW services. Using our Cloud First approach, legacy IT systems are converted to modern FedRAMP cloud service offerings. The Agency is implementing a Zero Trust Platform while adapting its IT security controls to function in the current pandemic telework environment. The agency is working with DHS CISA and OMB on our Zero Trust architecture, providing roadmaps and lessons learned for other Federal civilian agencies. The Agency will continue to pursue IT capabilities to meet EO 14028 while minimizing adverse impacts. The CIO Ratings highlight the impact of accepted risks with remaining legacy IT that limits FTC’s ability to fully implement technical capabilities while undergoing IT modernization.

Independent Assessment

We concluded, consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines , FTC's information security program and practices were established and maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. The overall maturity level of FTC's information security program was determined as Managed and Measurable, as described in the metrics annotated in this report. Accordingly, we found the FTC's information security program and practices were effective for the period of October 1, 2020, to September 30, 2021.

Initial Performance Summary

Gulf Coast Ecosystem Restoration Council

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

As a micro agency, GCERC has partnered with Federal Shared services to provide risk mitigation. The largest risk to GCERC is endpoint protection. GCERC is implementing the CISA CDM along with contracted services to provide endpoint protection and monitoring. In addition GCERC has procured TIC services to ensure secure Internet connections and monitoring for those connections.

Independent Assessment

The Department of the Treasury (Treasury) Office of Inspector General (OIG) contracted with an independent certified public accounting firm (Independent Assessor) to conduct an annual evaluation of the Gulf Coast Ecosystem Restoration Council's (Council) information security program and practices in support of the FISMA evaluation requirement. In its report, the Independent Assessor (IA), concluded that consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, the Council's information security program and practices were established and maintained for the five Cybersecurity Functions and nine FISMA Metric Domains. The IA found that the Council's information security program and practices were effective for the period July 1, 2020 through June 30, 2021. The overall maturity level of the Council's information security program was determined as Managed and Measurable based upon a simple majority of the maturity level for each of the domains. The IAs tests of effectiveness found no exceptions.

Initial Performance Summary

General Services Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	1	1
E-mail	4	3	16
External/Removable Media	0	0	0
Impersonation	0	1	0
Improper Usage	65	68	19
Loss or Theft of Equipment	0	0	0
Web	2	7	25
Other	24	22	21
Multiple Attack Vectors	0	0	0
Total	**96**	**102**	**82**

CIO Self-Assessment

FY21 continued trends from FY20 focusing on nation state threats manifesting itself via software supply chain and related attacks against widely used software solutions that affected so many in both Government and industry. GSA fully supports the Administration's goals to advance Zero Trust Architecture. We have taken deliberate actions moving GSA towards enterprise shared services, continued movement towards a shift left security model that prioritizes continuous innovation, continuous improvement, and DevSecOps. Risks and related mitigations faced in FY2021 are below:

1-Phishing: Continuous phishing campaign targeting GSA users and targeted groups; enhanced security awareness training; BOD 18-01 security; Email URL analysis and Executable sandboxing.
2-Hardware and Software Supply Chain: New Supply Chain and ICAM capabilities with dedicated office and governance processes including Executive Board for developing a strategy to coordinate activities and a Review Board for addressing prohibited articles;Technical and Operational processes to identify and prevent prohibited technologies including third party SCRM risk assessments of suppliers.
3-OT/IOT Security: Network segmentation to break out user and OT/IOT networks; Hardware/Software device testing via Device Testing Lab.
4-Malware and Cyber Hacking: Continued maturation of key technologies including but are not limited to: Enterprise Network Deception;Automated Red and Blue Team;Vulnerability Disclosure Policy and Bug Bounty;24x7x365 Security Operations Center;Tiered Incident Response ;Enterprise Logging with machine learning;Cyber threat hunting.
5-Remote Work Security: VPN Load Balancing;External DNS

Independent Assessment

For the Independent Audit on the Effectiveness of the U.S. General Services Administration’s (GSA) Information Security Program and Practices for fiscal year (FY) 2021, our scope included assessing the maturity levels for the FY 2021 IG FISMA Reporting Metrics and testing the NIST 800-53 security controls referenced in these metrics at the entity level, for 5 selected GSA operated information systems, and for 5 selected contractor information systems. In addition, we followed up on the status of 9 prior-year FISMA findings. Based on the work performed in FY 2021, we assessed the overall GSA IT security program as effective based on determining the mode of the individually assessed maturity levels for the 66 metrics, as directed by the FY 2021 IG FISMA Reporting Metrics guidance. Specifically, we assessed the Identify, Protect, Detect, and Respond Cybersecurity Functions as Optimized (Level 5), while the Recover Cybersecurity Function was assessed as Consistently Implemented (Level 3). While GSA did close the 9 prior-year findings, during our FY 2021 independent FISMA audit, we identified 6 new findings in the Protect Function that were consolidated into 4 findings in the FY 2021 report (1 in the Configuration Management FISMA Metric Domain and 3 in the Identity and Access Management FISMA Metric Domain). The nature of these findings did not affect our overall assessment of the Protection Function after determining the mode of the 30 Protect metrics. To improve its information security program, GSA should design, implement, and monitor qualitative and quantitative key performance indicators to measure the effectiveness of its contingency planning controls, processes, and activities. GSA should also develop and implement Plans of Action and Milestones (POA&Ms) to remediate the four FY 2021 audit findings.

Resolver solution; EDR solutions; threat monitoring dashboard for DDOS, VPN usage, and security threats.
6-Cloud Security: Deployment of new cloud security tooling to ensure the security of workloads in containerized spaces at run-time, visibility and control of delivery pipelines, and service mesh.

Initial Performance Summary

Department of Health and Human Services

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	19	23	106
E-mail	603	798	1,507
External/Removable Media	2	0	88
Impersonation	5	0	42
Improper Usage	4,674	3,493	3,188
Loss or Theft of Equipment	575	326	475
Web	609	91	2,232
Other	1,088	2,501	797
Multiple Attack Vectors	33	11	0
Total	**7,608**	**7,243**	**8,435**

CIO Self-Assessment

The cybersecurity threat landscape at HHS, the federal government, and the Healthcare and Public Health (HPH) Sector continues to evolve and grow increasingly complex. HHS' cybersecurity program has evolved as well, and remains able to best protect the Department from those threats and assist the HPH sector in mitigating the risks from those threats. HHS continues to mature its Cybersecurity and Enterprise Risk Management (ERM) integration with a Cyber-ERM group for thought-leadership and information sharing across HHS and its Operating Divisions. The High Value Asset (HVA) Program implemented additional security measures to ensure HVAs are prioritized based on risk impact and mission functionality. In FY21, HHS sent 901,181 phishing emails with an HHS resistance rate above 90%; reviewed 124,766 URLs and reported 13,924 malicious websites for takedown; analyzed 51,133 reported spam messages, 1,238 of which were malicious and 109 of which triggered malicious site takedown requests; researched 110 coordinated malspam campaigns; identified COVID-19 themed credential harvesting emails; investigated typosquatting domains where actors registered new domains mimicking well-known, legitimate domains. HHS continues to collaborate within HHS and its federal partners including the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to develop options for enhanced cyber hygiene, threat detection, and information sharing; HHS also released over 30 new cybersecurity awareness products to improve resiliency and drive behavior change in the HPH sector. Additionally, HHS continues to respond to Executive Order 14028, Improving the Nation's Cybersecurity requirements including reports on multifactor authentication, data encryption; zero trust and cloud technology strategies; HVAs and data sensitivity; and EO-critical software.

Independent Assessment

Through the evaluation of FISMA metrics, it was determined that the HHS's information security program was 'Not Effective'. This determination was made based on a number of competing factors including: (1) the evaluation of HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas, (2) the deficiencies identified across all functional areas, (3) HHS not identifying mitigating processes associated with ratings below Managed and Measurable for each control domain that would allow HHS to have an effective program, and (4) the evaluation of a maturity level below Consistently Implemented for individual metric questions both at HHS overall and at selected OpDivs. HHS is cognizant of opportunities which arise to strengthen the overall information security program which would help ensure that policies and procedures in place at all OpDivs are consistently implemented and in line with the requirements across their security programs. Two significant areas preventing HHS from achieving an effective program are in the ISCM and CP domains. For other areas evaluated as consistently implemented, HHS should define risk-based metrics to measure the effectiveness of their program in the domains of: Risk Management, Configuration Management, Identity & Access Management, Data Protection and Privacy, Security Training, and Incident Response. These metrics should be based on a central risk reporting process and appropriate toolsets being deployed to provide HHS with the necessary information to make informed cybersecurity risk decisions. These steps will help HHS achieve its mission through an effective and coordinated information security program.

Initial Performance Summary

Department of Housing and Urban Development

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	15	3	8
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	14	20	12
Loss or Theft of Equipment	0	0	0
Web	1	0	0
Other	11	15	10
Multiple Attack Vectors	1	0	0
Total	**42**	**38**	**30**

CIO Self-Assessment

This summary highlights the steps that the Department of Housing and Urban Development (HUD) has undertaken in Fiscal Year (FY) 2021 to mitigate and prevent cybersecurity risks to create a cyber safe Agency. In FY 2021, HUD has continued to take significant measures to inform HUD employees of the dangers of cyber vulnerabilities and risks of remote work through the increase in monitoring for cybersecurity awareness, conducting targeted personnel trainings, and facilitating malware and phishing campaigns. Specifically, the measures were performed through the enterprise wide Telework Cyber-Safety Awareness Campaign, FY 2021 Phishing Exercises, and the Ransomware IR/Contingency Planning tabletop exercise for OCIO. In the past 12 months, HUD has initiated a Data Loss Prevention (DLP) Program and enabled new data classification functions to prevent external sharing of data that could potentially contain sensitive information. Overall, HUD has closed 163 OCIO and Privacy aligned audit recommendations, operationalized three Cyber Dashboard domain views, and developed/updated more than 25 policies, procedures, and templates that address the spectrum of HUD's risk management process. In the upcoming Fiscal year, HUD is looking to improve upon its current cybersecurity posture through the expansion of trained and cyber-aware staff, enhancements of data protection capabilities, transition to NIST 800-53 Revision 5, and maturation of cybersecurity related capabilities.

Independent Assessment

The Department of Housing and Urban Development's (HUD) information security (IS) program was evaluated as not effective. HUD remained at the overall maturity of consistently implemented in FY 2021. HUD's information security continuous monitoring program (ISCM) saw significant improvements in FY 2021. HUD began implementing a revised process for ongoing authorizations (OA) and monitoring them under the continuous monitoring dashboards. Continued momentum to meet their defined timelines for OA and ISCM may be a strength and increase their maturity in future years. Challenges, such as incomplete and inaccurate system, component, and user account inventories; limited visibility and control of personally identifiable information; lack of processes for risk-based allocation of resources, and the lack of an implemented identify and access control program contributed to an ineffective information security program. HUD OCIO had successes in implementing a security operations center, however delays in meeting full operating capacity hindered the program from achieving an increased maturity. Throughout FY 2021, HUD created remediation plans for, took corrective actions on, and successfully closed many prior year HUD OIG recommendations. Continued emphasis on implementing and enforcing policies and procedures are essential for HUD to achieve an effective IS program. OIG recommends that HUD continue to prioritize its IS program by focusing on assessing and maturing the FISMA domains using a continuous and accountable approach.

Initial Performance Summary

Inter-American Foundation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	2
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**2**

CIO Self-Assessment

The IAF successfully tested and implemented 'Continuity of Operations' and 'Disaster Recovery" in the cloud.
The IAF agency has implemented a rogue detection device for monitoring and connecting to the agency network. The IAF is in the process of developing Supply Chain Plan and Policy.
The IAF has implemented the 'Continuous Diagnostics and Monitoring' through DHS.

Independent Assessment

IAF’s information security program was evaluated as part of the FY 2021 FISMA Audit. The FISMA Audit conducted by RMA included an evaluation of four out of five FISMA reportable systems at IAF. The audit determined IAF’s maturity level to be Consistently Implemented. Based on IAF’s overall implementation of security controls and considering the unique mission, resources, and challenges of IAF the independent auditors deemed IAF’s information security program as effective.

Initial Performance Summary

International Boundary and Water Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Defined
Detect	At Risk	Ad Hoc
Respond	Managing Risk	Consistently Implemented
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	**0**	**1**	**0**

CIO Self-Assessment

The International Boundary and Water Commission, U.S. Section (USIBWC) consist of 1 moderate General Support System (GSS) and 2 high Supervisory Control and Data Acquisitions (SCADA) operational systems. All information security programs comply with laws and regulation established by FISMA, as amended, and standards prescribed by the OMB and NIST. The USIBWC is in the process of reauthorizing a security assessment and authorization for its GSS, Nogales International Wastewater Treatment Plant (NIWTP) and South Bay International Wastewater Treatment Plant (SBIWTP) Supervisory Control and Data Acquisition (SCADA) systems. The agency anticipates a renewed GSS before the end of this calendar year. A renewed NIWTP and SBIWTP SCADA Authority to Operate (ATO) should be issued by the end of FY 2022. The agency was recently assessed by CISA and Department of State OIG. Recommendations and findings are currently under review. The agency is leveraging internal and contracted resources to obtain support required to address all recommendations. The Information Management Division (IMD) is in the process of updating its risk register and POAMs to reflect recent recommendations and findings from each cybersecurity assessment.

Independent Assessment

The Department of State Office of Inspector General (OIG) and OIG's independent contractor assessed the information security program of the International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC) as not effective for fiscal year (FY) 2021. The assessment scope included all three of USIBWC's major, Federal Information Security Modernization Act of 2014-reportable information systems. OIG's independent contractor found that USIBWC had taken steps to establish an organization-wide information security program by generally developing and implementing certain activities that support USIBWC's operations and assets. However, the assessment identified numerous areas where existing policies and procedures were not current and planned updates or development of new policies and procedures were in draft and not finalized during the scope period. The assessment resulted in 19 new recommendations, as well as a determination that 26 of 30 recommendations from previous FISMA audits remained open as of FY 2021.

Initial Performance Summary

Institute of Museum and Library Services

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	2	0
Multiple Attack Vectors	0	0	0
Total	**0**	**2**	**0**

CIO Self-Assessment

IMLS transitioned its General Support System (GSS) and other mission critical information systems to the cloud during FY 2020/2021. IMLS is operating under 100% telework mode since March 2020 due to COVID-19 pandemic and continued its policy to allow staff to securely access agency resources using their agency furnished devices as well as agency approved personal devices through VPN and multi-factor authentication. To further protect and enhance the security posture of the agency network which includes remote users, personal and agency furnished devices, and cloud-based assets, IMLS is implementing Zero Trust Architecture in compliance with the "Executive Order on Improving the Nation's Cybersecurity." Currently, IMLS Zero Trust Architecture implementation is in pilot phase and a comprehensive roll out across the agency is planned for FY2022. IMLS is also actively ensuring a PIV compliant workforce. Additionally, to mitigate cyber security threats against sensitive data, IMLS prioritized evaluation of the types and sensitivity of agency's controlled unclassified data (CUI) and performed a comprehensive analysis of data processing and storage solutions. The agency risks associated with exposure to and recovery from ransomware, malware, viruses and other cyber threats have been assessed. With comprehensive security controls, monitoring, real-time data and application backups, the agency is well positioned to defend and recover from cyber threats. IMLS provided a report to the Secretary of Homeland Security through the Director of CISA and to the Director of OMB. The report includes Identification of Sensitive Data, Data Classification Process, and Threats to Sensitive Data. IMLS is scheduled to establish a uniform policy to designate, safeguard, disseminate, and dispose CUI data in FY2022. In FY2021, IMLS has initiated a comprehensive security assessment and

Independent Assessment

The scope of this audit covers the Institute and Museum Library Services. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of Information Security Continuous Monitoring, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other areas as required by the FY2021 IG FISMA reporting Metrics. The results of the assessment were used to measure the maturity of the agency's information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels in which IMLS implements an information security program, develops, and disseminates sound policies and procedures, deploys automated mechanisms in support of risk management and data protection, and trains its personnel to maintain and institutionalize good security practices.
Conclusion:
Upon completion of the audit, it is apparent that IMLS has gone through extensive efforts in securing the organization IMLS environment and has complied with most security control requirements tested during the security assessment of the organization's information security program and information systems. The IMLS information security program was found to be implemented effectively due to the following factors validated by operational evidence:

- Information Security Continuous monitoring processes are well implemented and meet security requirements.
- Automated mechanisms are employed to support FISMA requirements for the Access Control, ISCM, and Configuration Management programs.
- IMLS ensures that Security training is monitored and provided to its stakeholders at least annually and given to personnel.

IMLS Contingency Plan executed 12/2019 with success.Due to authorization of its Information Systems by an independent assessor, to be completed by Q2/Q3 FY2022.

pandemic and agency wide remote work order updates to this document is in progress.

Initial Performance Summary

International Trade Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	2	1
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	4	1	1
Multiple Attack Vectors	0	0	0
Total	**6**	**3**	**2**

CIO Self-Assessment

Over the past few years, the Commission was worked to embrace telework and a mobile workforce. Numerous technologies like a PIV authenticated VPN, remote datacenter, O365 mail, Microsoft Teams, WebEx, GoTo Meeting, Virtualization, and Software-as-a Service cloud solutions have been implemented to support the remote workforce. These technologies, along with an IT service desk designed with a remote service model in mind, and business unit procedures and policies that enable a productive remote work environment placed the Commission in a good position to handle the expansion of telework under the COVID-19 national emergency. Because of this foresight and planning, the Commission did not need to make wide-scale changes to manage risk associated with COVID-19 related remote work. One key initiative that was undertaken to reduce risk associated with increased remote work was the enablement of a non-PIV FIPS 140 cryptographic multi-factor authentication option for remote user VPN connections. This allowed the Commission to support remote user VPN connections in situations where the PIV card is not an option (new users, temp staff, etc). In the past these non-PIV users were unable to connect the Commission's VPN.

Independent Assessment

We have deemed the US International Trade Commission's (Commission) information security program effective. During the second year of remote work due to the ongoing COVID-19 pandemic, the Commission continued to effectively manage software across all compatible devices. It also identified and remediated vulnerabilities. The Commission continued to strengthen its technical controls in managing all hardware on the network and improve its incident response and contingency processes. The Commission has a strong security and awareness program, which trains all users on current cybersecurity threats involving social media, identity management, cloud application systems, and best practices for protecting a home network.

Initial Performance Summary

Japan-United States Friendship Commission

Framework	CIO Rating	IG Rating
Identify	High Risk	N/A
Protect	At Risk	N/A
Detect	At Risk	N/A
Respond	At Risk	N/A
Recover		N/A
Overall	**At Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

The Japan-U.S. Friendship Commission is a nano agency of four FTEs. We remain compliant with federal mandates to the best of size and budgetary authority.

Independent Assessment

Initial Performance Summary

Millennium Challenge Corporation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	2	2	0
Loss or Theft of Equipment	1	0	0
Web	0	0	1
Other	2	1	0
Multiple Attack Vectors	1	0	0
Total	**6**	**3**	**1**

CIO Self-Assessment

1. The COVID-19 restrictions for remote access to information systems continues to provide cybersecurity risks to the Millennium Challenge Corporation (MCC). These restrictions are caused expiring certificates on or Personal Identity Verification (PIV) access control solutions. The MCC is requesting users update their PIV certificates on a limited basis using available PIV kiosks.
2. Operational necessities require the use of split tunneling for end-point access to the Internet. The Millennium Challenge Corporation mitigates this risk with by enforcing an application allow-list, which restricts authorized applications to an approved managed list. In addition, MCC has increased monitoring and end-point detection capabilities.

Independent Assessment

MCC's information security program was evaluated as part of the Fiscal Year (FY) 2021 FISMA Audit. The FISMA Audit conducted by RMA included an evaluation of four out of seven FISMA reportable systems at MCC. The audit determined MCC's maturity level to be Managed and Measurable. Therefore, the independent auditors deemed MCC's information security program as effective.

Initial Performance Summary

Morris K. Udall Foundation

Framework	CIO Rating	IG Rating
Identify	At Risk	N/A
Protect	At Risk	N/A
Detect	At Risk	N/A
Respond	At Risk	N/A
Recover		N/A
Overall	**At Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

UDALL continues to make cybersecurity the highest priority. All ED's and BOD's were addressed and where required, reported on in FY21. An independent FISMA was conducted in FY21 and work to address the identified deficiencies continues. UDALL's goal is to complete steps to get a security ATO in place and meet all requirements outlined in EO 14028 in FY22.

Independent Assessment

Initial Performance Summary

Marine Mammal Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Optimized
Protect	At Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Optimized
Overall	**At Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

The Marine Mammal Commission is a micro agency consisting of three Commissioners and nine members of the Committee of Scientific Advisors on Marine Mammals, all of whom are special government employees, supported by a staff of 14 full-time government employees. The Commission's office is located in Bethesda, Maryland. The Marine Mammal Commission does not own or manage any information systems. Any Personally identifiable Information is collected only for necessary purposes and is secured. The main means of ensuring security of federal information are as follows: 1) The Commission does not originate, receive, or store classified information, either electronically or in hard-copy. The Commission has a suitably rated safe that is kept in a locked room for storing such information, if the need should arise. 2) The Commission's official personnel records are maintained by the General Services Administration, Commissions and Boards. Supervisor records are maintained in a locked metal cabinet in the office of the Commission's Chief Administrative Officer. The Chief Administrative Officer and the Executive Director are the only staff with access to those records. 3) In FY 2012 the Commission initiated the Managed Trusted Internet Protocol Service (MTIPS) to provide a Trusted Internet Connection (TIC). The Commission has signed the EINSTEIN Memorandum of Agreement with the Department of Homeland Security. 4) All agency computers have antivirus software installed.

Independent Assessment

The Marine Mammal Commission is a micro agency consisting of three Commissioners and nine members of the Committee of Scientific Advisors on Marine Mammals, all of whom are special government employees, supported by a staff of 14 full-time government employees. The Commission's office is located in Bethesda, Maryland.

The Marine Mammal Commission does not own or manage any information systems. Any Personally identifiable Information is collected only for necessary purposes and is secured.

The main means of ensuring security of federal information are as follows:

1) The Commission does not originate, receive, or store classified information, either electronically or in hard-copy. The Commission has a suitably rated safe that is kept in a locked room for storing such information, if the need should arise.

2) The Commission's official personnel records are maintained by the General Services Administration, Commissions and Boards. Supervisor records are maintained in a locked metal cabinet in the office of the Commission's Chief Administrative Officer. The Chief Administrative Officer and the Executive Director are the only staff with access to those records.

3) In FY 2012 the Commission initiated the Managed Trusted Internet Protocol Service (MTIPS) to provide a Trusted Internet Connection (TIC). The Commission has signed the EINSTEIN Memorandum of Agreement with the Department of Homeland Security.

4) All agency computers have antivirus software installed.

Initial Performance Summary

Merit Systems Protection Board

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	1	0
Loss or Theft of Equipment	1	2	0
Web	1	0	0
Other	1	1	3
Multiple Attack Vectors	0	0	0
Total	**7**	**4**	**3**

CIO Self-Assessment

In FY 2021, the Merit Systems Protection Board (MSPB) took several steps to strengthen its risk posture, its cybersecurity program, and to reduce security threats. The agency remains committed to decommissioning legacy equipment and operating systems, and we deployed new Windows 10 laptops to all employees in FY 2021 with real time monitoring through the cloud. We were able to remove all but 10 instances of Windows Server 2008 within our environment. In June 2021, the agency hired its first CISO to provide cybersecurity leadership, risk management, and program direction. MSPB updated its CDM implementation by transitioning to a cloud-based CDM platform in support of the DHS program update. The agency updated its IT strategic plan to include all provisions from EO 14028 including, but not limited to, encryption, Zero Trust architecture, multifactor authentication, and cloud adoption. MSPB also maintains reporting to comply with all BOD's, ED's and other DHS directives. The agency maintains an MOA with DHS for EINSTEIN services including weekly scans of our internet-accessible addresses and systems, weekly Cyber Hygiene, HTTPS, and Trustworthy Email reports. MSPB continued to attend weekly CISA CyberLiaison, SOC, and C-CAR calls, along with participating in the Small and Micro Agency CISO Council. The agency maintains all available IPSS services (TA, MEF, DSS) on our MTIPS circuit and are actively engaged with our ISP for regular maintenance and incident resolution to protect our security boundaries. MSPB modernized its external website to include being hosted on a modern cloud platform that has improved security, availability, and usability for the public. Annual computer security training resulted in 100% completion and was delivered to employees through an automated platform. MSPB remains on schedule to move its next-generation business application into production in

Independent Assessment

This report presents the results of the annual Inspector General (IG) audit of the Federal Information Security Modernization Act (FISMA) of 2014. DOI ISSLoB performed an assessment of the current implementation of the MSPB GSS. This audit report documents the results of the
independent reviews, analysis, and tests performed by DOI ISSLoB of operational evidence provided by MSPB to comply with the FY 2021 IG FISMA Reporting Metrics requirements.

MSPB underwent a security assessment from 09/13/21 to 10/29/21 based on FY 2021 IG FISMA Reporting Metrics provided by DHS and OMB. During this time, ISSLoB interacted with MSPB personnel and reviewed evidence and artifacts to assess the implementation of the MSPB
information systems. The FY 2021 IG FISMA Reporting Metrics included security controls and requirements for the following domains:

- Identify (Risk Management and Supply Chain Risk Management (SCRM))
- Protect (Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training)
- Detect (Information Security Continuous Monitoring)
- Respond (Incident response)
- Recover (Contingency Planning)

It is ISSLoB's professional opinion based on the results of the security assessment, MSPB has complied with some of security control requirements tested during the security assessment of the IMLS GSS and web applications. On a positive note, MSPB has made significant improvements to its overall security program. The organization migrated its system laptops from

January 2023 allowing MSPB to decommission a significant number of legacy applications and systems.

Windows 7 to Windows 10; updated its public website to include more security features; and lastly, migrated its hosting environment to the cloud.

MSPB remains committed to improving its overall security program and remediating the discrepancies and process improvements documented in Section 6.0 Findings and Recommendations.

Initial Performance Summary

National Archives and Records Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	1
Web	3	0	0
Other	7	2	6
Multiple Attack Vectors	0	0	0
Total	**10**	**2**	**7**

CIO Self-Assessment

Information Technology (IT) security has improved but remains a challenge for NARA. NARA information security policies, procedures, and practices provide adequate protections that are generally effective. However, in some cases they lack the formal processes necessary to ensure that policies and strategies are consistently implemented. Because of long standing risks in NARA IT security, Information Services (I) has declared IT security a material weakness in internal controls. NARA continues to improve its ability to protect the confidentiality, integrity, and availability of NARA resources. In FY 2021, NARA continued to make progress towards its system authorization goals and is on schedule to achieve authorization for 95% of their Moderate FISMA reportable systems in FY 2022. Seven of the ten remaining moderate systems have already gone through a security assessment, two are in progress, and one is scheduled to start in FY 2022. Additionally, NARA continues to improve its performance related to Information Security Continuous Monitoring, Strong Authentication (ICAM), and Advanced Network and Data Protections (ANDP) while simultaneously fulfilling the requirements set forth in the recent White House Cybersecurity Executive Order (Cyber EO) 14028 issued in May 2021. In responding to the Cyber EO 14208 requirements, NARA has effectively standardized its common cybersecurity contractual requirements, updated its Cloud Migration Plan, established a Zero Trust Architecture Plan, inventoried Critical Software and thoroughly evaluated NARA's unclassified data types and sensitivity levels within all NARA FISMA Reportable Systems.

Independent Assessment

While NARA's overall maturity level has not changed from last year, NARA did improve in three domains. NARA continues to stress its commitment to improving information security throughout the agency and is making steady progress to that end.

In FY2021, NARA continued its progress toward a more mature information security program, including the following:

- Enhancements were made to NARA's Cyber Security Framework Methodology to reduce inconsistencies previously.
- NARA has significantly strengthened its completion rate for the annual security awareness training.
- Improvements were made to NARA's security assessment and authorization documentation.
- NARA has strengthened its assignment of information system security officers to FISMA reportable systems.

However, to fully progress towards consistently implemented, NARA will need to address the weaknesses in its policies and procedures to ensure they are accurate, complete, consistent, and communicated to all information security stakeholders. Additionally, NARA needs to ensure:

- The security assessment and authorization process better adapt to risk level impacted changes.
- Information security weaknesses are more consistently documented, monitored, and closed.
- Multi factor authentication for access to NARANet is enforced agency wide.
- User account management processes related to documentation, account reviews, account monitoring and the separation process are strengthened.
- Privacy specific training requirements for individuals with responsibility for personally identifiable information is implemented.
- Configuration management plans, policies and procedures

are either developed or enhanced.

- System patch and configuration vulnerabilities are remediated in a timely manner, and improved processes are developed to address unsupported software.
- Hardware asset inventories are more effectively managed.

Initial Performance Summary

National Aeronautics and Space Administration

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	5	1
E-mail	7	11	46
External/Removable Media	0	2	34
Impersonation	0	0	4
Improper Usage	1,329	1,165	607
Loss or Theft of Equipment	15	3	288
Web	3	17	123
Other	108	417	91
Multiple Attack Vectors	6	6	0
Total	**1,469**	**1,626**	**1,194**

CIO Self-Assessment

NASA takes seriously its responsibility to ensure the secure use of information technology in support of its mission objectives. In FY21, NASA established a working group to facilitate the execution of all requirements in Executive Order 14028, Improving the Nation’s Cybersecurity, including developing plans for required initiatives, soliciting stakeholder inputs, and coordinating and overseeing the Agency-wide implementation of required security controls and enhancements. Additionally, NASA continued to improve its HVA A&A documentation and processes, resulting in greater visibility into HVAs’ security postures and improved RMA and CAP Goal scores. Further, NASA also made other technical and operational security enhancements, including completing the first phase of remediation efforts to prevent end-of-life and end-of-support systems from remotely connecting to NASA’s enterprise network; and moving all NASA center traffic behind Agency-level firewall policies, blocking more than 5 billion unauthorized connections per day.

Independent Assessment

During our FY 2021 evaluation, we assessed NASA's information security policies, procedures, and practices by examining four (4) of the Agency's information systems. In addition, we assessed the Agency's overall cybersecurity posture utilizing a variety of processes, procedures, and techniques that leveraged interviews with Agency representatives, along with the review of prior work performed by NASA, NASA OIG, and GAO. Further, we also evaluated NASA's progress in addressing deficiencies identified in prior FISMA evaluations and audits performed by the NASA OIG. We determined that information security continues to remain a challenge for NASA based on this evaluation and other reviews. While NASA continues to make progress in securing its networks and information systems, its cybersecurity program remains ineffective when assessed against OMB's model, which requires agencies to achieve a level 4 maturity (managed and measurable) to be considered effective. While NASA continues to make incremental improvements in its cybersecurity program, NASA information systems continue to remain vulnerable to internal and external cybersecurity threats.

Initial Performance Summary

National Council on Disability

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	High Risk	Optimized
Detect	At Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Optimized
Overall	At Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

There has been no Cybersecurity risks to the agency so therefore no steps have been needed to be taken.

Independent Assessment

NCD’s overall assessment is deemed effective because our risk management process identifies threats and vulnerabilities to our IT assets and establishes acceptable controls to reduce the likelihood of a security breach or violation. NCD's our objective for each system at NCD is to ensure that the following security objectives can be realized for their information:

- Confidentiality - Protecting information from unauthorized access and disclosure.

- Integrity - Assuring the reliability and accuracy of information and IT resources by guarding against unauthorized information modification or destruction.
- Availability - Defending information systems and resources to ensure timely and reliable access and use of information.

Initial Performance Summary

National Capital Planning Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	At Risk	N/A
Detect	Managing Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	2	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	0	2
Multiple Attack Vectors	0	0	0
Total	**4**	**0**	**2**

CIO Self-Assessment

The National Capital Planning Commission (NCPC) continues to operate in a remote working environment. Most staff work from home and monthly Commission meetings continue to be hosted online. With the rapid shift to remote work due to the pandemic, the NCPC took a risk-based approach and modified security measures to ensure continued business operations. These temporary modifications created gaps in the security program. In FY 2021, the NCPC has taken the following actions to mitigate these gaps. The network infrastructure was simplified to minimize the potential cybersecurity attack surface. The team consolidated the server infrastructure, which resulted in decommissioning 25% of the servers. A new software asset management tool was implemented and identified multiple variations of the same operating system. The team streamlined the number of operating systems making it easier to manage and troubleshoot endpoints.

Several key factors have converged to create a pivotal time for the NCPC to make bold decisions on the future of the agency’s IT infrastructure. Security is at the forefront of these network modernization decisions. At the end of FY 2021, the NCPC is working towards a full cloud deployment in accordance with the latest TIC 3.0 Reference Architecture and Zero Trust Architecture principles.

Independent Assessment

Initial Performance Summary

National Credit Union Administration

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	0	0
E-mail	3	5	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	0	1
Loss or Theft of Equipment	4	6	4
Web	0	0	1
Other	5	1	28
Multiple Attack Vectors	0	0	0
Total	**16**	**12**	**34**

CIO Self-Assessment

While NCUA made progress in 2021, the following key risk areas are the most significant:
1) Data Management Security: NCUA manages enterprise data as a strategic asset through its full lifecycle to include security, privacy, and records management. NCUA established a data loss prevention program set out to define data labels and corresponding protections.
2) Legacy Application Security: NCUA deployed a modern application in 2021 and will subsequently sunset its oldest legacy application in fiscal year 2022. NCUA has developed requirements and is conducting an alternatives analysis to replace four more legacy applications in the next two - five years.
3) Insider Threat: NCUA is exploring additional protections through User and Entity behavior analytics (UEBA) which will accelerate detection and response capabilities to monitor known threats and behavioral changes in user data, providing critical visibility to uncover user-based threats that might otherwise go undetected.

Independent Assessment

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) assessed the NCUA in all Function areas and underlying Domains identified in the FY 2021 IG FISMA Reporting metrics as they pertain to the review of a sample of five of the NCUA's information systems and its overall information security program. The NCUA has continued to strengthen its information security program during Fiscal Year (FY) 2021. Specifically, we determined the NCUA implemented an effective information security program by achieving an overall Managed and Measurable maturity level based on the FY 2021 IG FISMA Reporting Metrics. In addition, the NCUA addressed and closed sE▯▯▯▯▯▯▯11 recommendations from the FY 2020 FISMA report. Furthermore, the NCUA is in the process of addressing and resolving the five remaining recommendations from the FISMA 2020 report. NCUA's appetite for technology and information management risk is low with regard to cost-effective security, as the confidentiality, integrity and availability of systems, data and information is foremost. Although we concluded that NCUA implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted six weaknesses within the supply chain risk management, configuration management, identity and access management, and data protection and privacy domains of the FY 2021 IG FISMA Metrics and have made seven new recommendations to assist NCUA in strengthening its information security program.

The recommendations we are making in the OIG's FY 2021 FISMA report should help the NCUA continue to improve the effectiveness of its information security program.

Initial Performance Summary

National Endowment for the Arts

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Defined
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	3	0
Loss or Theft of Equipment	1	0	0
Web	0	0	1
Other	1	0	23
Multiple Attack Vectors	0	0	0
Total	**3**	**4**	**24**

CIO Self-Assessment

Primary cybersecurity risks to the National Endowment for the Arts (NEA) during FY21 include phishing emails and ransomware. Prior to FY21, the NEA already deployed solutions to mitigate these risks. The solutions include: web content filtering, email content filtering, and Data Loss Prevention (DLP). All machines are protected by centrally managed anti-virus and antimalware. Mobile devices are protected by a centrally managed mobile device management solution.

In FY21, the NEA has taken several steps to significantly improve cybersecurity capabilities to protect the confidentiality, integrity and availability of agency systems by continuing to adopt Zero Trust methodology. The NEA continued to move critical assets to FedRAMP approved cloud service providers. The agency is currently working with DHS on the implementation of the CDM tools. An identity access management system has been deployed with 80% of systems integrated. Security program reviews have demonstrated progress this year in improvement of the agency's security posture, and integration of tools that greatly improve cybersecurity incident monitoring, prevention, and response.

During the pandemic, the agency began the deployment of the new private access platform to replace the agency's VPN solution. This platform was fully deployed by the end of Q2FY21 and the VPN solution was retired. The agency has also implemented the use of a single sign-on authenticator for its 2factor authentication allowing the NEA to reach 100% PIV enablement.

Independent Assessment

Williams, Adley & Company-DC LLP (Williams Adley) assessed the effectiveness of the NEA's information security program in accordance with FISMA requirements and determined that NEA's information security program remains ineffective in FY 2021, as the NEA did not consistently implement its defined processes across all FISMA domains. Based on the assessment of NEA's information security program, the overall maturity level is Level 2, Defined. To achieve the next level of maturity, Williams Adley believes that the NEA needs to continue taking action to address previously issued recommendations.

Initial Performance Summary

National Endowment for the Humanities

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	1	0	0
Web	0	0	0
Other	0	5	3
Multiple Attack Vectors	0	0	0
Total	**1**	**5**	**3**

CIO Self-Assessment

For FY2021, the NEH continues to work around the COVID-19 pandemic challenges of diverting our IT department's resources to supporting 100% of the staff in full remote work. This included migrating the entire staff to secure file sharing into the cloud for the enterprise, refining onboarding policies and procedures, and integration of updated policies as part of NEH's Annual Security Awareness and Privacy training program. Even with resource challenges, NEH not only has maintained its security posture from last year, but have also made a few improvements to the capabilities within security domains from FY2020.

While the RMA Overall Summary page in FY2021 has not changed from FY2020, NEH has made improvements in several capabilities shown in the values and improved rating of the a few of the highest risk capabilities. For example:

FY20 risk: The CAP Goal for "A9. Exfiltration and Enhanced Defenses" capability to check traffic for unauthorized exfiltration was at 0%.
FY21 status: NEH's IT staff started the migration of NEH user data to cloud-based data storage, Microsoft One Drive and leveraged Microsoft monitoring capabilities increasing NEH's overall Exfiltration and Enhanced Defenses capability to check traffic for unauthorized exfiltration to 66%.

FY20 risk: NEH's Configuration and Vulnerability Management section where Systems assessed by SCAP products had 70% coverage with a rating of High Risk.
FY21 status: NEH's installation and use of the CDM Qualys SCAP tools increased the scanning of GFE endpoints to improve to an 89% with an improved rating of At Risk.

Independent Assessment

The NEH information security program has been designed to comply with NIST and FISMA requirements. Considering the small size of the agency, certain activities comprising the information security program are effective in providing continuous visibility into threats and risks to NEH information systems and data. However, foundational components of risk management (Identify), ISCM (Protect), and contingency planning (Recover) have not been fully implemented, and this condition impedes the overall effectiveness of the NEH information security program. NEH leadership has committed personnel and budgetary resources to support the completion of activities that will advance the agency's efforts to fully implement its risk management and ISCM programs. The accreditation and authorization (A&A) of one core information system is expected to be completed prior to the end of December 2021 and planning activities related to the A&A of a second core information system have started.

NEH’s CISO continued to utilize new Security Awareness and Privacy Training modules this year that was very well received by staff. This new training is much more engaging and the NEH anticipates it will result in an increase in staff knowledge of best cybersecurity practices.

NEH also continues work on several system reviews, including a review of various system ATO’s.

Initial Performance Summary

National Labor Relations Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	1
E-mail	0	0	2
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	4
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	1	6
Multiple Attack Vectors	0	0	0
Total	**2**	**1**	**13**

CIO Self-Assessment

In FY 21, the National Labor Relation's Board (NLRB) underwent a DHS/CISA assessment on its HVA systems in accordance with BOD 18-02, Securing High Value Assets. A total of 8 recommendations were derived from the assessment. The agency took immediate action and resolved 7 of the 8 risks with CyberDirectives. The one open finding is currently managed through the CyberScope portal with an expected completion date at the end of November, 2021. In addition, NLRB requested CISA perform a remote penetration test to evaluate the effectiveness of NLRB's controls for its internet facing systems. Zero critical findings were identified with only four (4) medium and one (1) low risks identified. NLRB took action to mitigate these findings.

NLRB FISMA reportable systems are regularly tested through an independent assessor. The have current PO&AM's and have valid ATO's. During the past year the Agency continued its transition into the cloud and now the majority of IT assets are located within the cloud. This past year we continued to develop, document processes and implement automated capabilities to protect the confidentiality, integrity and availability of agency resources. In FY 21, the agency maintain our Managed and Measurable rating during the annual FY 21 FISMA IG audit.

The Agency continued to protect their IT resources and has been especially diligent through this period of increased telework. NLRB actively monitors agency resources in real time utilizing cloud-based solutions. In addition, we also continued work with the CDM program to safeguard, secure, and strengthen our security posture. In conjunction with the CDM effort we have installed and are now utilizing new monitoring capabilities. The Agency took action and reported

Independent Assessment

Based upon the testing conducted by the outsider auditors, the OIG concurs with the FISMA calculated assessment rating of "effective." The scope of the review was Fiscal Year 2021. The OIG also notes that the NLRB OCIO implemented all prior audit recommendations related to information technology security.

all required information as directed by the EO 14028, Improving the Nations’ Cybersecurity. In addition, NLRB is 100% compliant with BOD 18-01 and has taken immediate action to all CISA ED's.

Initial Performance Summary

National Mediation Board

Framework	CIO Rating	IG Rating
Identify	At Risk	N/A
Protect	High Risk	N/A
Detect	At Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	At Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	1	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	1
Multiple Attack Vectors	0	0	0
Total	**1**	**1**	**1**

CIO Self-Assessment

The National Mediation Board continues to undertake initiatives towards meeting the CIO FISMA metric objectives. The agency's technical and security professionals are performing updates to the agency's security policies and procedures, identifying gaps, and have implemented several solutions to improve our overall security posture and compliance to the OMB, DHS, and FISMA requirements. Since the last reporting, the agency has deployed an enterprise endpoint vulnerability management and detection response solution (EDR), a new secure remote access system, published a new IT Security Policy, established a comprehensive user authorization process, defined secure configuration baselines, performed contingency and incident response test exercises, updated the internal network, performed over 10 assessments of shared services or third-party vendors to establish ATO/ATU status, and closed over 10 program level/Tier 1 Plans of Action and Milestones (POA&Ms). The agency has two major projects in process to be completed within FY22 - complete implementation of MTIPS and a new multi-factor authentication/PIV system. Additionally, continue with efforts underway to create or update organizational and system level policies and procedures to comply with NIST 800-53 Revision 5.

Independent Assessment

Initial Performance Summary

Nuclear Regulatory Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	6	5	7
Loss or Theft of Equipment	1	0	1
Web	0	0	2
Other	0	4	1
Multiple Attack Vectors	0	1	0
Total	**7**	**10**	**11**

CIO Self-Assessment

The NRC needs to protect itself from cybersecurity risks generated by malicious actors and catastrophic events that impact the confidentially, integrity, and availability of information systems and the agency's sensitive data. The NRC has used risk assessments to develop and implement a proactive strategy to identify and mitigate risk to the agency. These actions include successfully implementing the controls, activities, and assets required by the DHS CDM program. The agency has a fully staffed and trained SOC, IR team and skilled staff to implement, operate, and maintain assets. From a programmatic stance, the NRC adheres to a governance program that leverages FISMA 2014 and FITARA authorities and requirements and ensures that each system maintains an ongoing authority to operate. All cybersecurity role holders attend mandated annual training and all account holders take annual computer security training. A daily situational awareness report that contains prior day events, current system status, and emerging issues is distributed, reviewed, and discussed at regularly held meetings. The NRC SOC also uses a number of automated information services to ensure that we are up to date on threat intelligence data that helps the agency take a proactive approach to hunting unauthorized and potentially malicious behavior on our networks to be aware of issues and take action before they become events or incidents. The NRC regularly assesses its tool set against the evolving threat landscape and adapts as needed. The NRC continued to rapidly respond to the COVID-19 related telework environment; most notably in increased bandwidth capacity and modified patching processes to maintain an effective security posture on distributed computers. The NRC is aware of the risks facing the agency and takes the appropriate actions to ensure the information and information systems within remain secure. These steps and their results are

Independent Assessment

As the independent assessor our objective was to evaluate the effectiveness of the information security policies, procedures, and practices of the NRC. To achieve this objective, we evaluated the effectiveness of NRC's information security policies, procedures, and practices on a representative subset of the agency's information systems. We then determined whether NRC's overall information security program and practices were effective and consistent with the requirements of FISMA, DHS, and other federal regulations, standards, and guidance applicable during the evaluation period. While we determined that NRC established an effective Agency-wide information security program and practices, we identified a few weaknesses that may have some impact on the Agency's ability to adequately protect the NRC's systems and information. To be consistent with FISMA, the NRC should strengthen its information security risk management framework by addressing the follow summary level recommendations; 1) incorporate the use of its ISA into its SDLC, create cybersecurity risk profiles to prioritize risk responses, and complete the agency cybersecurity risk register, 2) improving privileged user access reviews and audit log activity reviews, and 3) coordinate contingency plan exercises with external stakeholders such as supply chain partners/providers.

reflected in the annual reports provided to OMB and DHS.

Initial Performance Summary

National Science Foundation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Optimized
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	1
E-mail	2	1	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	1
Loss or Theft of Equipment	0	0	0
Web	0	1	0
Other	1	3	2
Multiple Attack Vectors	0	0	0
Total	**3**	**5**	**5**

CIO Self-Assessment

The National Science Foundation's (NSF) security posture reflects its commitment to a secure environment and sustained improvement. NSF targets strategic areas for strengthening security and privacy programs. NSF's continuous monitoring program allows the Foundation to identify and evaluate risks and plan appropriate mitigations. Cybersecurity risks such as phishing, unauthorized access and data loss, and supply chain threats pose challenges to maintain a high secure posture. NSF protects its High Value Assets, through continuous monitoring, rigorous control reviews, risk assessments, vulnerability management and service recovery. NSF adopted advanced features of its advanced managed detection and intelligence-led incident response services to improve 24x7 Security Operations Center capabilities. NSF continues to focus on expansion of cloud capabilities to support secure, reliable, and highly available technology services. The Zero Trust Architecture (ZTA) framework provides a path for modernizing the environment as NSF extends mission critical applications into diverse cloud environments. NSF's implementation of ZTA is a long-term effort that will require coordinated plans across cybersecurity areas. NSF established a supply chain risk management policy and risk assessment process that provides approaches to mitigate potential risks in products, services, and solutions. NSF will continue to monitor all Framework functional areas and maintain focus on enterprise cybersecurity risk management for the Foundation’s high value assets.

Independent Assessment

To assess whether the National Science Foundation (NSF) effectively implemented its agency-wide Information Security Program and practices for FY 2021, Kearney & Company, P.C. (Kearney) conducted a performance audit on behalf of NSF-OIG. Kearney performed detailed testing of NSF’s Network General Support System (GSS) and United States Antarctic Program (USAP) GSS for compliance with selected National Institute of Standards and Technology (NIST) standards and other controls as specified in the FY 2021 Inspector General FISMA Reporting Metrics.

Based on our audit, NSF’s Information Security Program was effective for FY 2021. The driving factor for this assessment is the consistent implementation and application of NSF’s control environment, which has directly impacted NSF’s overall ratings. Improvements were achieved by developing and implementing corrective action plans in response to prior year deficiencies, however some deficiencies remain unremedied.

To become more effective, NSF should ensure it implements plans of action and milestones (POA&Ms) in a timely manner to address findings identified during this audit and other self-assessments.

The draft version of the metrics released on May 12, 2021, introduced the concept of a weighted average system where certain metrics are rated as a priority rating. We analyzed NSF’s metrics score on the weighted average system and determined that there would be minimal impact to the FISMA metrics with the weighted average system.

Initial Performance Summary

National Transportation Safety Board

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	3	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	2	0	1
Multiple Attack Vectors	0	0	0
Total	**5**	**1**	**1**

CIO Self-Assessment

NTSB has taken the following steps in FY2021 to mitigate cybersecurity risks. The first risk identified was lack of Multi-factor authentication. The Agency implemented a product that provided a customizable, secure, and drop-in solution to add authentication and authorization services to Agency applications. The second risk identified was active privilege accounts. All active privilege accounts identified in all Agency systems were disabled.

Independent Assessment

The scope of this audit covers the National Transportation Safety Board General Support System, Microsoft Office 365, Azure, and National Transportation Safety Board Laboratory. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of Information Security Continuous Monitoring, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other areas as required by the FY2021 IG FISMA reporting Metrics. The results of the assessment were used to measure the maturity of the agency's information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels in which NTSB implements an information security program, develops, and disseminates sound policies and procedures, deploys automated mechanisms in support of risk management and data protection, and trains its personnel to maintain and institutionalize good security practices.

Upon completion of the audit, it is apparent that NTSB has gone through extensive efforts in securing the organization GSS environment and has complied with most security control requirements tested during the security assessment of the NTSB information security program and information systems. The NTSB information security program was found to be implemented effectively due to the following factors validated by operational evidence:

- Agency wide policies and procedures have been developed documented and disseminated according to security control criteria requirements.
- Information Security Continuous monitoring processes are

well established by
assigning ISCM activities to NTSB stakeholders with defined frequencies and security requirements.

- Vulnerability scanning of agency information systems and assets has been established
and is performed according to FISMA security requirements and fr

Initial Performance Summary

Nuclear Waste Technical Review Board

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

For FY21 the predominate risks to the Nuclear Waste Technical Review Board (NWTRB) have been related to phishing and unauthorized access attempts to cloud-based services by foreign actors. NWTRB has continued to update its processes and infrastructure to strengthen resistance to these risks. Multifactor authentication has been integrated for all users accessing our remote systems. Additionally, conditional access policies have been implemented to further limit access to NWTRB resources. Security awareness and phishing training has been given to all users with routine reminders issued throughout the year. Phishing exercises were conducted to test user responses which revealed a 0% user click rate. NWTRB has continued to maintain sound cyber-hygiene practices using internal CDM, auditing, DHS shared services, and regular patching of all information systems. In FY21 NWTRB possessed zero Critical or High vulnerabilities older than 7 days on any server or workstation and had no information security, cyber incidents, or breaches. NWTRB continues to prioritize the need for sound cybersecurity practices using assessments to identify areas of strength, improvement, and then executing based on those findings.

Independent Assessment

During the period between August 11, 2021 and September 10, 2021 an independent assessor performed an independent security assessment on the Nuclear Waste Technical Review Board (NWTRB) Infrastructure General Support System (GSS). The independent security assessment of the NWTRB Infrastructure GSS was conducted in accordance with (IAW) National Institute of Standards and Technology (NIST) guidelines, FY21 FISMA Metrics, Office of Management and Budget (OMB) Memorandum M-21-02, Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements and NWTRB Board IT Security Policy requirements. In accordance with the above guidance and the Independent Security Assessment Plan, the security assessment team developed and implemented test procedures to assess stated requirements of the SSP. These procedures included visual inspections, and reviews/analyses of system documentation. Testing was designed to obtain an accurate representation of the system in its current environment. These documented procedures served as a starting point for testing to ensure that all security policy objectives and vulnerabilities are examined. The methodology used by the independent assessor consisted of Threat Identification, Vulnerability Identification, Risk Analysis, Corrective Action Recommendation, and Results Documentation. Overall NWTRB GSS continued to improve its maturity in FY21 by increasing maturity ratings in the areas of Risk Management, Configuration Management, Identify and Access Management, Data Protection and Privacy, Security Training, ISCM, and Contingency Planning. The only functional area with maturity score that went down in FY21 was Incident Response, which was due to the increased weight of two metrics. Additionally, the assessment team noted several Plan of Actions and Milestones (POA&Ms) were closed in the last year. NWTRB will continue to pursue further improvement through the maturity model levels to best protect agency systems.

Initial Performance Summary

Office of the Comptroller of the Currency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	10	5	4
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	3	0	1
Multiple Attack Vectors	0	0	0
Total	**13**	**5**	**5**

CIO Self-Assessment

To address cybersecurity risks to the agency, the OCC has in FY 2021 continued to prioritize developing cybersecurity awareness in its highly mobile workforce, delivering weekly phishing exercises to promote user awareness of secure email practices and implementing an external email warning banner to reduce instances of misdirected emails. It implemented endpoint controls expanding its off-network policy enforcement to enhance security controls on user endpoints. The OCC continues to implement federal guidance and executive orders to the fullest extent possible. For example, it implemented the vulnerability disclosure policy required by DHS Binding Operational Directive 20-01 to encourage external researcher reporting of vulnerabilities in its external-facing systems, and has integrated these discoveries into its vulnerability management policy and processes. The OCC continues to leverage its identity and access management and cloud access security broker technologies for its deployment of cloud systems and services as part of its cloud-smart strategy.

Independent Assessment

For the FY 2021 FISMA Unclassified performance audit, the independent auditor assessed the effectiveness of OCC's bureau-level information security controls that align to the FY 2021 IG FISMA Reporting Metrics for the period July 1, 2020 through June 30, 2021. Where relevant, the assessor tested these in-scope information security controls for IT Management General Support System and its sub-system, eDocs. OCC's test results and the in-scope bureaus' results were aggregated and considered into Treasury's overall unclassified FISMA performance audit results. The independent auditor followed the Generally Accepted Government Auditing Standards in conducting the FY 2021 performance audit.

Initial Performance Summary

Office of Government Ethics

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	1
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	2
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**3**

CIO Self-Assessment

In FY 2021, OGE engaged assessors from the Enterprise Services Center, Information Security Assessment Group, Federal Aviation Administration, to conduct an independent assessment of the OGE Network using FY 2021 FISMA Chief Information Officer (CIO) metrics. Twenty-nine (29) moderate findings were identified by the assessor. No “very high” or “high” findings were identified. Nine (9) of the findings are covered by signed risk acceptances. For three (3) of those weaknesses, the assessor downgraded the residual risk from "Moderate" to "Low." Consequently, the OGE Chief Information Officer (CIO) will write sixteen (16) Plans of Action and Milestones (POAMs) and three (3) Risk Acceptances (RAs) to address outstanding moderate findings. Each finding will documented, assigned an ID, and monitored until mitigated or accepted by the Authorizing Official (AO). Each POAM will be signed by the CIO and the AO to indicate either closure or risk acceptance.

Also in FY 2021, OGE engaged assessors from the U.S. Department of the Interior to conduct an independent assessment of its information security program using FY 2021 FISMA Inspector General (IG) reporting metrics. The purpose of this audit was to determine the effectiveness of the agency’s information security program and practices. This was OGE's third annual audit against these requirements. Previous audits created a solid baseline from which OGE was able to work. FY2021’s audit results showed continuous improvement, even in the face of challenges placed upon OGE by new requirements and the COVID-19 pandemic. For purposes of the Audit, FY2021 IG FISMA Reporting Metrics and NIST Cybersecurity Framework identified five domains. These domains are measured against five maturity model levels: ad hoc, defined, consistently implemented, managed

Independent Assessment

The scope of this audit covers the Office of Government Ethics. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of Information Security Continuous Monitoring, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other areas as required by the FY2021 IG FISMA reporting Metrics. The results of the assessment were used to measure the maturity of the agency’s information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels in which OGE implements an information security program, develops, and disseminates sound policies and procedures, deploys automated mechanisms in support of risk management and data protection, and trains its personnel to maintain and institutionalize good security practices.

Upon completion of the audit, it is apparent that OGE has gone through extensive efforts in securing the organization GSS environment and has complied with most security control requirements tested during the security assessment of the OGE information security program and information systems. The OGE information security program was found to be Managed and Measurable; notwithstanding, the 1 discrepancy described in section 6.

and measurable, and optimized. The high-level result of OGE’s FY 2021 IG FISMA Metrics Audit was “Managed and Measurable” in all domains.

Initial Performance Summary

Office of Navajo and Hopi Indian Relocation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	Managing Risk	N/A
Detect	Managing Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**1**

CIO Self-Assessment

1. The Agency determined that the Information Technology (IT) policies, procedures, and processes required updating to maintain IT governance over Agency IT resources. In response the Agency has completed the following updates:

- Updated System Security Plan for the Agency's General Support System (GSS).
- Updated eighteen (18) IT policies and procedures.
- Updated mission-critical IT assets listing.

2. The Agency determined that IT resources (e.g., laptops, desktops, servers) had unnecessary software. In response the Agency has completed the following tasks:

- Removed all software/applications that were necessary for mission operations.
- Initiated process for developing a configuration baseline for all IT resources.
- Implemented an Information System Continuous Monitoring (ISCM) program.
- Implemented a patch management process to assist in hardening IT resources.

3. The Agency determined that auditing processes for IT resources (e.g., laptops, desktops, servers) lacked automation. In response the Agency has completed the following tasks:

- Procured software that provides the capability to perform automatic logging, vulnerability reports, and risk assessment reports.

4. The Agency determined that PIV cards were not being used regularly in mission operations. In response the Agency has performed the following tasks:

- Initiated testing of PIV cards for use during all mission operations (where applicable), specifically for the email system.

5. The Agency determined that IT infrastructure required

Independent Assessment

compliance with EIS and TIC mandates. In response the Agency has performed the following tasks:

- Initiated procurement of hardware and software components to implement a more secured IT environment.

Initial Performance Summary

Office of Personnel Management

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Defined
Detect	Managing Risk	Defined
Respond	Managing Risk	Managed and Measurable
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	4	0	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	156	167	193
Loss or Theft of Equipment	10	9	0
Web	0	0	0
Other	57	32	67
Multiple Attack Vectors	1	0	0
Total	**228**	**208**	**261**

CIO Self-Assessment

The agency has continued its efforts to enhance its cybersecurity posture and infrastructure through technology modernization and policy and procedure updates as well as expanded and enhanced cloud utilization. The Fiscal Year began with the technical separation of DCSA information systems from OPM. Improvements continued with widespread device replacements, significantly reducing unsupported operating systems in the environment. OPM's past and current modernization efforts continued to ensure a secure and smooth telework environment at OPM. The agency continues to report and collaborate on responses to White House Executive Orders while maintaining routine reporting, maintenance and auditing activities.

Independent Assessment

The FY 2021 FISMA IG Reporting Metrics use a maturity model evaluation system derived from the NIST Cybersecurity Framework. The Cybersecurity Framework is comprised of five “function” areas that map to the nine “domains” under the function areas. These nine domains are broad cybersecurity control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. Each domain is comprised of a series of individual metrics, which are the specific controls that we evaluated and tested when assessing the agency’s cybersecurity program. Each metric receives a maturity level rating of 1-5.

This year, we used the new pilot concept of calculating the weighted average of metric’s maturity levels to determine the domain maturity levels.

This year we requested OPM to conduct a self-assessment. This gave OPM the opportunity to document its current maturity level for each metric and the maturity level that it hopes to achieve by the end of FY 22. We validated OPM’s stated/current maturity level throughout the fiscal year and reported on the results of our analysis.

Risk Management - Maturity Level 2; SCRM - Maturity Level 1; Configuration Management - Maturity Level 2; Identity, Credential, and Access Management - Maturity Level 2; Data Protection and Privacy - Maturity Level 2; Security Training - Maturity Level 3; Information Security Continuous Monitoring - Maturity Level 2; Incident Response - Maturity Level 4 and Contingency Planning - Maturity Level 2.

In FY 2021, OPM's cybersecurity maturity level is measured as 2 - Defined.

Level 4, Managed and Measurable, is considered to be an effective level of security for the overall program level. Therefore, the information security program is deemed ineffective. Recommendations have been provided to assist in elevating the program's overall level and can be found in the comments sections for specific metric.

Initial Performance Summary

Office of Special Counsel

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Consistently Implemented
Detect	Managing Risk	Consistently Implemented
Respond	Managing Risk	Consistently Implemented
Recover		Consistently Implemented
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	2	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	2
Multiple Attack Vectors	0	0	0
Total	**2**	**0**	**2**

CIO Self-Assessment

OSC's information system does not contain any HVAs. OSC made great strides during fiscal year FY21 by creating documented processes and procedures to reduce overall risk. OSC received an overall risk rating of Low in its most recent security assessment. OSC continues to monitor its information system using a variety of security tools to identify and resolve all system anomalies.

Independent Assessment

OSC has gone through extensive efforts in securing its GSS environment and has complied with most security control requirements tested during the security assessment of the OSC information security program and information systems. The OSC information security program was found to be implemented effectively due to the following factors validated by operational evidence:

- Most of OSC's security policies and procedures have been developed, documented and disseminated according to security control criteria requirements.
- Information Security Continuous monitoring processes are well established by assigning ISCM activities to OSC stakeholders with defined frequencies and security requirements.
- Vulnerability scanning of agency information systems and assets has been established and is performed according to FISMA security requirements and frequencies.
- OSC has established an effective configuration management program for its information systems.
- OSC ensures that Security training is conducted at least annually.

Initial Performance Summary

Occupational Safety and Health Review Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Ad Hoc
Detect	Managing Risk	Ad Hoc
Respond	Managing Risk	Ad Hoc
Recover		Consistently Implemented
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	2	3
Multiple Attack Vectors	0	0	0
Total	**0**	**2**	**3**

CIO Self-Assessment

OSHRC assessment of the cybersecurity risks to the agency originate from our existing collaborative relationships with IPSS(Einstein), CDM Dashboard, MISA, US-Cert scans, as well as internal endpoint clients and system firewall appliances. During FY2021, OSHRC mitigation efforts have purely been in a reactive/proactive approach as risks are identified. Based on notifications from the many monitors in place, OSHRC evaluates the relevance of the risks against existing systems and reacts accordingly as to risk being present and whether a preemptive action is necessary. OSHRC has not had a violation as a result of a cybersecurity risk in FY2021.

Independent Assessment

Agency has implemented practices in place in each area but primary factors are no formalized strategies and procedures for the operations currently in place for ISCM, Risk Management. Metrics and lessons learned are also items done in practice but not formalized. So operational practices are in place to support an EFFECTIVE overall rating.

Initial Performance Summary

Pension Benefit Guaranty Corporation

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	2	2
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	**4**	**2**	**2**

CIO Self-Assessment

Cybersecurity has been, and will continue to be, a top management priority at PBGC as technology and threat landscapes evolve. In FY21, PBGC made significant progress in strengthening its information security program through the ongoing alignment of cybersecurity policies and procedures with the functional areas outlined in the NIST Cybersecurity Framework (CSF) and corresponding FISMA performance measures. As a result, this led to improved implementation of previous audit recommendations and management of cybersecurity and privacy related risks. PBGC's information security program was evaluated as effective, evident through eight (8) of the nine (9) security domains within the IG FISMA metrics surpassing effective thresholds. These efforts will continue to be prioritized as PBGC works to sustain effective cybersecurity capabilities to identify, prioritize, and manage cyber risks across its enterprise.

While the Corporation has met FY21 targets for the CIO and IG FISMA metrics and related Cybersecurity Cross-Agency Priority (Cyber CAP) goals, it recognizes the need to address recently published CISA Binding Operational Directives (BODs) and newly identified key points of Executive Order 14028, which includes zero trust architecture (ZTA), supply chain risk management, and integrating modernized cloud security solutions. PBGC will continue to be attentive toward the information disseminated via CISA and OMB to ensure the Corporation remains agile in the rapidly changing threat environment. FY22 cybersecurity program planning will focus on FISMA compliance,

Independent Assessment

The PBGC OIG contracted with an independent auditor to determine the degree of compliance for PBGC's information security programs and practices with FISMA requirements, DHS reporting requirements, and applicable OMB and NIST guidance. This audit assessed the maturity of PBGC's information security program using the FY 2021 IG FISMA metrics under OIG oversight. Based on a sample of six systems, the independent auditor noted improvements in all five Cybersecurity Framework functions. PBGC raised the assessed maturity of the Identify, Protect and Contingency Planning functions to managed and measurable bringing the overall information technology security program to an effective level. All five functions were assessed as effective at Managed and Measurable. In the new supply chain risk management domain, PBGC developed a strategy but additional attention is needed to mature this new domain to an effective level. Our detailed report and recommendations will be available in our audit report of PBGC's FY 2021 compliance with FISMA.

with an emphasis on CSF maturation and the Corporation’s risk management assessment (RMA), to secure the confidentiality, integrity and availability of information systems and data. Additional priorities and enhancements will be captured in the FY22 Enterprise Cybersecurity and Privacy Policy Roadmap. PBGC is committed in its efforts to continuously improve and mature its cybersecurity posture.

Initial Performance Summary

Privacy and Civil Liberties Oversight Board

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

Cybersecurity risks to the Privacy and Civil Liberties Oversight Board's (PCLOB) information assets include maintaining the availability and integrity of agency and partner data, which enables the Board's oversight and advisory functions and facilitates coordination with key stakeholders. The Board has made steady progress towards implementing NIST controls to mitigate risks to IT assets, environment, and mission-critical functions from cyber attacks. The Board procured Security Operation Center (SOC) services to enhance network visibility and response efforts. The FY 2021 independent audit validated the Board's efforts rating the PCLOB controls as effective. The independent audit identified three controls for remediation. Also, the Board achieved Full compliance with DHS ED BOD's 21-04, 21-03, and 21-01 and suffered no major information security incidents in FY 2021. Additionally, the Board strengthened its security posture and situation awareness by implementing capabilities to detect vulnerabilities and mitigate attacks. The Board conducted an independent security pen-test and phishing exercise to identify and resolve gaps. The Board will continue to leveraged shared service providers along with DHS CDM, and Managed Trusted Internet Protocol Service providers to identify and contain threats and prioritize risks.

Independent Assessment

The information security program of the Privacy and Civil Liberties Oversight Board was evaluated as effective. The PCLOB does not have an internal IG and has contracted with an independent auditor to conduct the FISMA IG Assessment. The PCLOB is proactive in remediating all identified deficiencies and strengthening existing security controls. The results of the FY 2021 independent audit identified three findings for selected controls. The PCLOB has develop POAM's to remediate the auditors findings. PCLOB had four findings for FY 2020 and no findings in FY19. The PLCOB also commissioned (2) two independent vulnerability assessments of its IT infrastructure in FY21 to gauge the effectiveness of its information security program. The resulting report stated that information systems exhibits “a better than average external and internal vulnerability profile” indicating effective implementation FISMA security controls. The PCLOB has fully implemented MTIPS across the enterprise and continues to steadily increase their security posture across all cybersecurity CAP goal targets.

Initial Performance Summary

Postal Regulatory Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	At Risk	N/A
Detect	At Risk	N/A
Respond	At Risk	N/A
Recover		N/A
Overall	At Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	1
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**1**

CIO Self-Assessment

During this past year, the Commission continued to take steps to improve the overall security and performance of its systems and IT Infrastructure.

- Updated and improved its Continuity of Operations Plan (COOP) and developed a Pandemic Response Plan (PRP) in response to the impact of the COVID-19 pandemic. Both plans were created to ensure that the Commission has a plan for continuity of the Commission's essential functions across a wide range of potential emergencies.
- Transitioned all employees from personal equipment to government-furnished laptops to support secure remote work.
- Completed first formal Security Assessment & Authorization (SA&A) on the Commission's network which resulted in an Authority to Operate (ATO). As part of the assessment, a number of weaknesses were identified which resulted in security findings called Plan of Actions and Milestones (POA&Ms). Identifying and remediating POA&Ms is ongoing and further strengthens the Commission security posture.
- Published a Vulnerability Disclosure Policy that allows researchers to test outward facing websites and contact us if any issues are identified.
- Migrated all employee mail boxes into Microsoft's O365's SaaS Exchange environment and enable extra services such as Teams, in response to on-premise exchange vulnerability.
- Implemented the CDM shared service tool, Qualys, for its vulnerability scanning, SWAM, and HWAM capabilities, working closely with the DHS CISA CDM team. Since the tool has been in place the IT team has reduced vulnerabilities by 30%.
- Advanced compliance with HSPD-12 by starting process of obtaining and implementing PIV cards for all employees that will be used in multi-factor authentication.
- Fully implemented DISA STIG configuration settings on all

Independent Assessment

Commission laptops and workstations which includes an automated mechanism to prevent the usage of untrusted removable media.

- Completed successful migration of network to new MTIPS provider.

Initial Performance Summary

Presidio Trust

Framework	CIO Rating	IG Rating
Identify	At Risk	
Protect	At Risk	
Detect	Managing Risk	
Respond	At Risk	
Recover		
Overall	**At Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	3	3	2
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	1	3	0
Web	0	0	0
Other	1	1	0
Multiple Attack Vectors	0	0	0
Total	**5**	**7**	**2**

CIO Self-Assessment

In FY21, the Presidio Trust advanced its security and privacy program in several significant ways. We completed Business Continuity plans for all critical processes and systems. We addressed methods of preventing and responding to our most common incident type, email phishing. We documented an incident response checklist/playbook.

We aligned our resources to respond to several federal emergency directives, initiatives and executive orders. We investigated and mitigated several high-profile vulnerabilities in our environment. Our newly-developed vulnerability disclosure program will enable external security researchers to responsibly report vulnerabilities in our systems to us. We began our journey to a Zero-Trust Architecture, including selection of a multi-factor authentication solution and piloting with IT staff and participants from each division of our agency. Data center environmental monitoring was improved, which proved to be instrumental during an equipment failure. Lastly, we formed a strategy to group and prioritize our systems and perform control assessments. Assessments were performed on the 2 highest priority system groups - high value assets and Internet-facing systems.

Independent Assessment

Initial Performance Summary

Railroad Retirement Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Defined
Protect	Managing Risk	Defined
Detect	Managing Risk	Ad Hoc
Respond	Managing Risk	Defined
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	21	10	4
Loss or Theft of Equipment	18	16	5
Web	0	0	0
Other	20	0	8
Multiple Attack Vectors	0	0	0
Total	**59**	**26**	**17**

CIO Self-Assessment

The adequacy and effectiveness of this Agency's information security policies, procedures, and practices is progressing as directed by OMB, the Department of Homeland Security (DHS), the National Security Council (NSC) staff, and the CIO Council as reflected in the RRB's Inspector General (IG) FY 2021 metric report. The RRB will continue to make incremental steps to reach the overall maturity goal of Level 4 - Managed and Measurable. Specifically, the RRB plans on continuing to improve the security posture of the agency's high value assets, improve the RRB's TIC 3.0 and ICAM strategy, and improving the RRB's patch management program. Additionally, the agency is in the process of upgrading our current EDR solution to Microsoft Defender MDE, we are participating the the CDM SSP 2.0 program and are progressing towards meeting the requirements for MFA and encryption from EO 14028.

Independent Assessment

To assess how the Railroad Retirement Board (RRB) established and implemented its agency-wide Information Security Program and practices, as required by the Federal Information Security Modernization Act of 2014 (FISMA), our independent auditors performed detailed testing of the RRB's Agency Enterprise General Information System (AEGIS), Benefit Payment Operations (BPO), Financial Management Integrated System (FMIS), and Financial Interchange (FI) systems and applications for compliance with selected controls from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, Security and Privacy Controls for Federal Information Systems and Organizations. Overall the Information Security Program was ineffective with each of the five NIST Cybersecurity Domains (CSF) rated at "Level 2 – Defined." This a notable improvement from fiscal year (FY) 2020 for the Identify, Detect, and Recover domains, which were rated at "Level 1 - Ad Hoc." This improvement is attributed to the RRB's allocation of resources to update policies and procedures and a commitment to improving the agency's information security processes across all domains. However, continued management attention is necessary in all functions, as the RRB Information Security Program is rated below "managed and measurable," which is deemed to be an effective level of security in the FISMA CSF maturity model.

Initial Performance Summary

Small Business Administration

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	4	43	145
E-mail	1,100	1,694	772
External/Removable Media	6	0	0
Impersonation	7	37	268
Improper Usage	134	494	245
Loss or Theft of Equipment	6	7	33
Web	139	415	612
Other	368	238	1,536
Multiple Attack Vectors	1	1	9
Total	**1,765**	**2,929**	**3,620**

CIO Self-Assessment

The SBA built, delivers, and continues to mature resilient and robust Enterprise Cybersecurity Service (ECS) capabilities that can be consistently implemented, maintained, and leveraged throughout the agency. These ECS capabilities align to the President's Management Agenda (PMA) Cross Agency Priority (CAP) Goals and cover area such as cyber threat intelligence, network monitoring, penetration testing, risk management and assessment, vulnerability scanning and remediation, event log correlation, awareness training, and incident response.

Delivered at the enterprise level, the ECS capabilities allow the SBA to better support the Small Business Community by providing consistency of process, ensuring broad visibility, and facilitating efficiency through program offices' ability to consume a single solution.

Institutionalization of these services continues to result in a steady increase in the agency's CAP Goal Metrics and OMB Maturity Ratings over a multiyear period. These ECS capabilities make the SBA well-positioned to align to the EO 14028 initiatives; enabling the SBA to rapidly respond to recent well-publicized global cyber events with minimal impact and no indications of compromise.

Independent Assessment

The information security program of the Small Business Administration (SBA) was evaluated as not effective. Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, we evaluated the design, implementation, and operating effectiveness of SBA's information security policies, procedures, and practices. We determined that SBA has established and maintained its information security program and practices for the nine FISMA metric domains. In general, SBA's ratings were consistent from the previous year although additional weaknesses were identified with systems the agency stood up to support the CARES Act and other programs supporting economic relief due to the COVID-19 pandemic. In addition, SBA was rated as "Ad Hoc" for supply chain risk management because policies and procedures over the program were not yet mature, although management is continuing to focus more on this program and strengthen it for fiscal year 2022. SBA also maintained the rating of its incident response program as "Managed and Measurable" and is operating in an effective manner. However, other than the incident response program, the other eight domains of the program reflected deficiencies that we identified were rated not effective. SBA has worked to implement recommendations from previous FISMA reports. We acknowledge CARES Act processing requirements continue to greatly challenge the security posture of SBA, and we also recognize challenges remain in implementing an effective IT security program for the agency.

Initial Performance Summary

Securities and Exchange Commission

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	0	1
E-mail	249	13	1
External/Removable Media	0	1	0
Impersonation	0	0	0
Improper Usage	57	37	69
Loss or Theft of Equipment	0	0	0
Web	24	2	0
Other	61	5	44
Multiple Attack Vectors	4	0	1
Total	**396**	**58**	**116**

CIO Self-Assessment

During FY 2021, the Securities and Exchange Commission (SEC) continued to make progress toward improving its information security program amidst continued challenges presented by the pandemic. The SEC enhanced security awareness and training efforts, improved vulnerability mitigation capabilities, and further improved incident detection and management capabilities. The SEC conducted quarterly phishing exercises for all personnel and assigned supplemental training to those personnel identified by exercises as susceptible to phishing. Multiple third parties, including DHS, conducted penetration testing, architecture reviews, and other risk assessment activities to identify vulnerabilities and test incident response mechanisms. The SEC's Office of Information Technology (OIT), in partnership with business owners, completed security assessment and authorization activities for fifty FISMA reportable systems. OIT also facilitated the remediation of over three-hundred eleven self-identified deficiencies consisting of POA&Ms associated with the SEC's assessments of its network infrastructure and major applications. The SEC completed corrective actions sufficient to close twenty-six prior year information technology (IT) related Office of the Inspector General (OIG) audit recommendations and five IT related Government Accountability Office (GAO) audit recommendations.

Independent Assessment

Despite facing continued unique challenges presented by Coronavirus Disease 2019 (COVID-19), including the significant increase in telework, the U.S. Securities and Exchange Commission (SEC) has made progress in improving its information security program by refining its management of security training roles and responsibilities, enhancing its security training strategy and security awareness training, implementing the agency's policy for specialized security training, improving its software asset inventory tracking, implementing a Vulnerability Disclosure Policy (VDP), refining it's configuration management processes related to reconciliation of software code in production, and improving its incident response and contingency planning capabilities. While the SEC made program improvements, the agency faced challenges with developing a Supply Chain Risk Management program, managing its Federal Information Processing Standard Publication 199 documentation for its information systems, implementing strong authentication mechanisms for privileged and non-privileged users, and the utilization of lessons learned in its Information Security Continuous Monitoring practices. As a result, Kearney & Company, P.C. (Kearney) determined that the SEC's information security program did not meet the definition of "effective".'

Initial Performance Summary

Social Security Administration

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	267	241	204
E-mail	90	42	31
External/Removable Media	5	3	1
Impersonation	13	43	2
Improper Usage	1,462	2,386	1,215
Loss or Theft of Equipment	35	41	26
Web	560	1,800	1,859
Other	2,353	4,305	2,956
Multiple Attack Vectors	11	17	16
Total	**4,796**	**8,878**	**6,310**

CIO Self-Assessment

SSA's mission requires it to collect PII for over 325 million Americans. This information is vital to performing the agency's essential functions but makes its network, systems, and databases a rich target for adversaries. Protecting our networks and the information we use to administer our programs remains a critical priority. In FY 2021, we made efforts to expand our component engagements and ensure appropriate awareness of cyber risks and compliance. During this unprecedented time of adapting our networks and workforce to support increased telework in response to the COVID-19 pandemic, we maintained a high level of assurance within our cybersecurity program while continuing to provide critical services to the American public. Specifically, in the Identify area of the NIST framework: we implemented our Information System Security Officer program to strengthen compliance and adherence to federal and agency security requirements. In the Protect area: We continued our mitigation efforts surrounding unauthorized software to include policy enforcement; removing instances of unauthorized software from our network; implementing a block list for non-business and potential malicious software. In the Detect area: we improved our Information Security Continuous Monitoring strategy to incorporate changes to process and technology, brought about in part by our efforts to implement DHS' Continuous Diagnostic and Mitigation program capabilities, and to make informed risk-based decisions. In the Respond area: we successfully demonstrated an effective and mature incident response program through our handling of multiple cyber attacks. In the Recover area: we continued providing guidance related to continuity of operations in the Emergency Management Handbook. This information aligns with directives and standards issued by Department of Homeland Security, Federal Emergency Management Agency,

Independent Assessment

Although SSA established an Agency-wide information security program and practices, our Independent Public Accountant (IPA) identified several deficiencies related to Risk Management; Supply Chain Risk Management; Configuration Management; Identity and Access Management; Data Protection and Privacy; Security Training; Information Security Continuous Monitoring; Incident Response; and Contingency Planning. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. In addition, our IPA assessed only one Federal Information Security Modernization Act of 2014 domain as Managed and Measurable (Level 4). The Fiscal Year 2021Federal Information Security Modernization Act of 2014 Inspector General Reporting Metrics defines an effective information security programs as Managed and Measurable (Level 4).

Occupational Safety and Health Administration, and General Services Administration.

Initial Performance Summary

Selective Service System

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

The Office of the Chief Information Officer (OCIO) for Selective Service System continued to mature its IT modernization plan in FY 2021. The agency responded to Executive Order (EO) 14028 by developing and implementing a Cloud Strategic Plan and Cloud Roadmap that aligned with the Federal Cloud Smart Strategy and its three pillars: security, procurement and workforce.

SSS also upgraded network MTIPS and MPLS infrastructure and increased network bandwidth to enhance security cloud applications architecture, posture/prepare the agency for a Microsoft O365 cloud migration.

In FY21 SSS also deployed CISCO Adaptive Security Appliance (ASA) Next Generation Firewall for internal firewall segmentation enhancing the agency's network security posture with an advanced defense in depth and zero trust architecture approach to cybersecurity. This Next Generation Firewall gave us application filtering, identity based ACL's, and advanced real time IDS/IPS functionality. SSS also matured its VPN security posturing to scan GFEs before access to the network.

In FY 2021, Selective Service migrated away from a commercial wireless network provider and implemented a secure agency-wide enterprise-class wireless network solution.

Through coordination and partnership with the Department of Homeland Security (DHS) during FY 2021, the Selective Service System upgraded the Continuous Diagnostics and Mitigation (CDM) Shared Services Platform 1.0 to the Shared Services Platform 2.0. The upgrade allowed the Selective Service System to streamline the cloud strategy and move away from two on-premise security applications to two cloud hosted state-of-the-art next generation security applications that are part of the CDM share services offering.

Independent Assessment

The scope of this audit covers the Selective Service System. DOI ISSLoB performed an assessment of the effectiveness and level of implementation of Information Security Continuous Monitoring, Contingency Planning, Incident Response, Data Protection and Privacy, Identity and Access Management, Configuration Management, Security Training, Risk Management, and other areas as required by the FY2021 IG FISMA reporting Metrics. The results of the assessment were used to measure the maturity of the agency's information security processes on a maturity model spectrum developed by DHS and OMB. This maturity model provides the foundation levels in which SSS implements an information security program, develops, and disseminates sound policies and procedures, deploys automated mechanisms in support of risk management and data protection, and trains its personnel to maintain and institutionalize good security practices. Upon completion of the audit, it is apparent that SSS has gone through extensive efforts in securing the organization GSS environment and has complied with most security control requirements tested during the security assessment of the SSS information security program and information systems. The SSS information security program was found to be implemented effectively.

Initial Performance Summary

Department of State

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	10	6	2
E-mail	1,043	289	18
External/Removable Media	1	1	2
Impersonation	0	3	0
Improper Usage	609	631	559
Loss or Theft of Equipment	8	3	7
Web	158	110	13
Other	495	192	181
Multiple Attack Vectors	52	16	6
Total	**2,376**	**1,251**	**788**

CIO Self-Assessment

The Department of State 2021 Annual FISMA Report demonstrates the Department's continued efforts to improve IT security by prioritizing and aligning initiatives with EO 14028. The Department is investing in a Zero Trust architecture, expanding the number of systems utilizing secure cloud capabilities, and implementing Multi-Factor Authentication (MFA) and encryption of data-at-rest and data-in-transit across the enterprise. The Department is also establishing the NIST Supply Chain Risk Management Framework to identify critical software and secure IT hardware and software purchases in order to further enhance the Department's IT security environment. State plans to continue refining and implementing risk management indicators, developing cybersecurity governance policies, and collaborating with partners across the Federal Government to guide investment and leadership decisions and enhance the overall cybersecurity posture.

Focus areas for improvement that will need to be supported in the coming Fiscal Year include both short-term (one year effort) and long-term (multi-year effort) remediation actions. The Department has authorized 87% of high impact systems at this time and expects to have this metric at 100% by FY 2022 Quarter 02 in April 2022. Similarly, the Department has attained 87% authentication of High Value Asset (HVA) systems and anticipates having metric at 100% by FY 2022 Quarter 02 in April 2022. Other areas of focus include improving (1) authorization of moderate impact systems currently at 63%, (2) HVA encrypted data-at-rest currently at 37% encryption, and (3) HVAs reconfigure or disable upon detection of a security violation currently at 23%. While improvements in statistics are likely to occur in the next fiscal year, these efforts will require multi-year attention.

Independent Assessment

The Department of State (Department) Office of Inspector General (OIG) and OIG's independent contractor assessed the information security program of the Department as not effective for fiscal year (FY) 2021. The assessment scope included a selection of the Department's major, Federal Information Security Modernization Act of 2014-reportable information systems. OIG's independent contractor found that the Department had taken steps to establish an organization-wide information security program by generally developing and implementing certain activities that support the Department's operations and assets, as well as designating a new position, the Enterprise Chief Information Security Officer, during FY 2021, to centrally discharge the Department's cybersecurity responsibilities. However, the assessment identified numerous areas where controls and processes could be improved. The assessment resulted in 18 new recommendations, as well as a determination that 27 of 36 recommendations from previous FISMA audits remained open as of FY 2021.

Initial Performance Summary

Department of State Office of Inspector General

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	Managing Risk	Optimized
Respond	Managing Risk	Optimized
Recover		Optimized
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	9	37
Loss or Theft of Equipment	0	3	4
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**12**	**41**

CIO Self-Assessment

The Department of State OIG network and major applications support its mission to conduct independent audits, inspections, evaluations, and investigations to promote economy and efficiency and to prevent and detect waste, fraud, abuse, and mismanagement in the programs and operations of the Department of State and the US Agency for Global Media. While OIG employs a defense-in-depth cybersecurity strategy to prevent and mitigate threats, residual risks from threats such as spear phishing, malicious web sites, insider threats, and zero-day threats persist.

OIG took several actions in FY 21 to mitigate cybersecurity risks and bolster defenses. OIG implemented additional cybersecurity policies to improve sensitive data protection and increase accountability for cybersecurity incidents. OIG authorized and implemented several new security and governance tools to improve OIGNet security posture and meet compliance requirements, including a document and labeling protection solution and enhanced mobile threat defense. OIG tested and implemented additional controls on endpoints to further protect against malware and unauthorized activity as well as conditional access policies to alert and block sign-in attempts with high-risk attributes.

OIG also completed a zero trust pilot for remote users utilizing the TIC 3.0 use cases and completed a plan for further adoption of zero trust principles as required by Executive Order 14028. OIG sustained its participation in the CDM program and implemented CDM Phase I tools provided by CISA.
OIG increased its cybersecurity user outreach and continued phishing exercises to ensure all staff remain vigilant of current threats. OIG met its FY 21 phishing goal with a less than 10%

Independent Assessment

As independent auditors, we conducted 2021 IG FISMA Metrics Assessment and determined that OIG regularly reviews, updates and shares its policies and procedures utilizing OIG Compass hosted on Microsoft SharePoint Intranet Site, consistently implements the security controls, manages and measures through effective metric reporting, and deploys automation, where necessary and safe, to support sustainable continuous monitoring and cybersecurity practice. There were no significant deficiencies found during the audit. During interview sessions as well as review of artifacts and collected evidence, we noted effective cybersecurity and integrated enterprise risk management practices, demonstrating optimization and continuous improvement in virtually all domain areas, including “Incident Response”. OIG followed through with 2020 IG FISMA Metrics recommendations to implement advanced technologies over these past 12 months that have added visibility and alerts for cyber, operations and helpdesk teams to collaborate, and contain risks, both for on-premises, and cloud environment. FY2021 IG FISMA Metrics audit reflected solid cybersecurity and risk management frameworks. We identified areas of improvement through recommendations as OIG continue to manage innovation, efficiency, automation, continuous monitoring and human skills in an evolving threat landscape. OIG has implemented a comprehensive, defense-in-depth architecture to be effective and exceed OIG mission expectations.

click-rate. OIG received a rating of “Managing Risk” on the FY21 Q2 Risk Management Assessment and Level 5 Optimized maturity ratings for the FY 2021 IG FISMA metrics.

Initial Performance Summary

Surface Transportation Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Ad Hoc
Protect	At Risk	Defined
Detect	Managing Risk	Defined
Respond	At Risk	Defined
Recover		Defined
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	8	4
Multiple Attack Vectors	0	0	0
Total	**0**	**8**	**4**

CIO Self-Assessment

The STB welcomes is pleased to report that the Board's overall information security program continues to improve, year over year, as reflected in the FY21 FISMA audit report. This improvement reflects the STB's commitment to implementing a cost-effective, risk-based security program that is aligned with the National Institute of Standards and Technology (NIST) security standards and guidelines. The STB's focus has been to continue its IT system modernization strategy through the adoption of the cloud. The STB has also gained additional vulnerability management, hardware asset management, and software asset management capability through government provided shared services.

Independent Assessment

For the FY 2021 audit, we evaluated STB's information security program and practices based on a representative sample of its information systems: specifically, the General Support System (STB-GSS) and two cloud-based systems (AtHoc and Dynamic Case Management System (DCMS)). The FY 2021 audit covered the period from October 1, 2020 to July 31, 2021. Based on the audit procedures performed, we concluded that STB's information security program remains ineffective as the agency continues to make progress in maturing its overall information security program through the development of its policies and procedures to address prior year recommendations. While STB has made significant efforts to address previously identified issues, additional work is needed to define and implement an effective information security program.

In summary, eight (8) recommendations were closed. Furthermore, Williams Adley issued twenty-seven (27) new recommendations to support STB's efforts to define and implement its information security program and processes. At the conclusion of the FY 2021 audit STB's information security program was rated at a Level 2, Defined.

Initial Performance Summary

Department of the Treasury

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	4	2
E-mail	54	7	2
External/Removable Media	1	1	0
Impersonation	6	0	0
Improper Usage	14	139	154
Loss or Theft of Equipment	10	5	3
Web	3	1	2
Other	54	49	80
Multiple Attack Vectors	0	0	1
Total	**142**	**206**	**244**

CIO Self-Assessment

The mission of the Department of the Treasury is to maintain a strong economy and promote conditions that enable economic growth and stability at home and abroad; strengthen national security by combating threats and protecting the integrity of the financial system; and manage the U.S. government's finances and resources effectively. To execute its mission, Treasury must store, process, transmit, and share large volumes of sensitive financial and personal information affecting the transaction of trillions of dollars. Treasury faces cybersecurity risks inherent in its interactions with private and other public sector organizations, limitations of authentication technologies, reliance on externally managed critical infrastructure, and current lack of centralized visibility of agency information technology assets and networks.

The likelihood of risk realization is magnified by the expansion of telework and continuing evolution in the volume, sophistication, and frequency of cyber threats. Treasury leadership remains engaged in the development of plans to address these risks. Throughout FY 2021, Treasury continued to leverage investments from supplemental funding provided through the Cybersecurity Enhancement Account to mitigate cybersecurity risks. In order to proactively address increased risks, Treasury continued to develop the Enterprise Cyber Risk Management program to include cybersecurity Supply Chain Risk Management to manage vulnerabilities that can be exploited to affect Treasury assets, especially critical under increased telework.

In FY 2021, Treasury achieved or exceeded CAP goal targets in nine of 10 areas. This achievement is attributed to increased Treasury-wide collaboration and clarifying guidance to improve reporting. Treasury remains committed to providing appropriate protection of our critical information and systems including maintaining an overall rating of "Managing Risk" on

Independent Assessment

The Department of the Treasury Office of Inspector General (OIG) contracted with an independent certified public accounting firm, Independent Assessor (IA), to conduct an annual evaluation of the Treasury's information security program and practices for its unclassified systems and Collateral National Security Systems (NSS). The scope of the IA's work did not include the Internal Revenue Service (IRS), as that bureau was evaluated by the Treasury Inspector General for Tax Administration (TIGTA).

Unclassified: The IA concluded that Treasury established and maintained its information security program and practices for its unclassified systems for the 5 Cybersecurity Functions and 9 FISMA Metric Domains. However, the IA determined that the program was ineffective, according to DHS criteria, as reflected by the 10 unclassified findings noted within 4 of the 5 Cybersecurity Functions and within 7 of the 9 FISMA Metric Domains. The IA made 22 recommendations related to these control deficiencies.

Collateral: The IA concluded that Treasury established and maintained its information security program and practices for its Collateral NSS for the 5 Cybersecurity Functions and 9 FISMA Metric Domains. However, the IA determined that the program was ineffective according to DHS criteria and as reflected by the 5 deficiencies noted within all 5 of the Cybersecurity Functions and within 8 of the 9 FISMA Metric Domains program areas. The IA made 11 recommendations related to these control deficiencies.

TIGTA: The IRS's Cybersecurity Program was generally aligned with applicable FISMA requirements, OMB guidance and NIST standards and guidelines. However, due to program the OMB Cybersecurity Risk Management Assessment (RMA).

components that were not at an acceptable maturity level, the Cybersecurity Program was not fully effective. TIGTA did not make any recommendations as part of its annual FISMA evaluation and reports only on the level of performance achieved by the IRS using the guidelines for the applicable FISMA evaluation period

Initial Performance Summary

Tennessee Valley Authority

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	2	0
External/Removable Media	0	1	0
Impersonation	1	0	0
Improper Usage	2	3	4
Loss or Theft of Equipment	4	14	17
Web	0	0	2
Other	15	1	0
Multiple Attack Vectors	1	0	0
Total	**23**	**21**	**23**

CIO Self-Assessment

Cybersecurity remains the top risk to the TVA enterprise. TVA met the challenges by increasing the number of cybersecurity personnel with the proper skillset to be experts and leaders in the cybersecurity industry. TVA led a cyber response team as part of the Defense Advanced Research Projects Agency Rapid Attack Detection, Isolation and Characterization Systems recovery exercise to restart a hacked US electric grid. In December 2020, it was discovered that SolarWinds Orion products were being exploited by malicious actors through a compromise in the supply chain. TVA mitigated the SolarWinds risk by identifying impacted systems, implementing an Incident Response Team and shutting down the impacted systems until a fix is available. When a water treatment plant was the victim of a cyberattack, TVA led a training event with the Federal Bureau of Investigation and local power companies on the attack and the Colonial Pipeline attack. TVA responded to Executive Order 14028 Strengthening the Nation’s Cybersecurity and formed response teams. TVA's Continuous Diagnostics and Mitigation (CD&M) Program continues to mature. The CD&M Agency dashboard is receiving data from asset management and identity and access management tools and services. The CD&M Operational Technology deployment is in Study Phase to evaluate tools and services. TVA was protected by enhancing email security protections agency-wide and deploying new endpoint protections. Security behaviors of TVA employees and contractors were tested by phishing exercises. TVA experienced problems with remote access to TVA systems over the Memorial Day weekend. It was determined TVA was being bombarded with requests with the intent to deny service to TVA resources. TVA responded to these attacks by implanting a geolocation blocking standard and utilizing a third-party load shedding service to diversify the

Independent Assessment

Based on the analysis of the metrics and associated maturity level defined by fiscal year (FY) 2021 IG FISMA metrics, we found TVA's information security program was operating in an effective manner. In addition, analysis of the Detect and Recover Functions resulted in improvements for this year. FISMA requires each agency's IG to conduct an annual independent evaluation to determine the effectiveness of the information security program and practice of its respective agency. The audit objective was to evaluate TVA's information security program and agency practices for ensuring compliance with FISMA and applicable standards, including guidelines issued by OMB and NIST. Our audit scope was limited to answering the FY 2021 IG FISMA metrics.

response and to load-shed the bombardment of requests at TVA’s edge.

Initial Performance Summary

United States Access Board

Framework	CIO Rating	IG Rating
Identify	Managing Risk	N/A
Protect	Managing Risk	N/A
Detect	Managing Risk	N/A
Respond	Managing Risk	N/A
Recover		N/A
Overall	Managing Risk	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**0**

CIO Self-Assessment

United States Access Board (USAB) continues to strengthen its information security policies and processes by identifying areas in its security posture for improvement. Some actions taken in FY21 include adopting controls in preparation of NIST 800-53 rv5 adoption, improved privacy controls and policies, TIC 3.0 security assessment.

In the process of shifting baseline security from NIST 800-53 rv4 to NIST 800-53 rv5, USAB privacy and security have worked closely together to ensure policy alignment that meets the needs of the agency in preparation for ATO reassessment in FY22. In addition, the agency has performed an in-depth assessment against TIC 3.0 to improve security strategy, architecture, and visibility. In FY22 the agency will complete TIC 3.0 implementation, improve ICAM strategies, and re-assess the security baseline against NIST 800-53 rev5.

Independent Assessment

Initial Performance Summary

United States Agency for Global Media

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	2	1	2
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	5	4	9
Multiple Attack Vectors	0	0	0
Total	**8**	**5**	**11**

CIO Self-Assessment

Starting on October 25, 2021, OIG released the FY 2021 FISMA audit report, which reflects the agency's improvements across several FISMA domains, as well as the agency's improved overall information security program maturity level to level 3, "consistently implemented." The report documents how, over the past year, USAGM has made remarkable improvements in information security despite challenges the COVID-19 pandemic presented to the agency's IT operations. Notable accomplishments include:

- Deployment of tools and processes to improve our Information Security Continuous Monitoring Program;
- Enactment of USAGM Multi-factor Authentication solutions;
- Implementation of established policies and procedures - specifically within the Risk Management, Security Training, and Incident Response domains, in which USAGM achieved a maturity rating of "Managed and Measurable;"
- Continued implementation of the agency's Enterprise Risk Management framework and Information Security Risk Management strategy; and
- Development of a Supply Chain Risk Management Strategy, Policy, and Program Plan.

While USAGM has made a great deal of progress over the past year, I also recognize that we must do more. I will ensure my staff are working to continuously improve the agency's information security program and to achieve FISMA compliance.

Independent Assessment

The Department of State Office of Inspector General (OIG) and OIG's independent contractor assessed the information security program of the U.S. Agency for Global Media (USAGM) as not effective for fiscal year (FY) 2021. The assessment scope included a selection of USAGM's major, Federal Information Security Modernization Act of 2014-reportable information systems. OIG's independent contractor found that USAGM had made significant progress in establishing an organization-wide information security program by generally developing and implementing activities that support USAGM's operations and assets. However, the assessment identified areas where planned improvements or development of new activities and controls were not finalized during the scope period. As such, the OIG used its discretion and assigned a level 3, consistently implemented, maturity for the agency's overall rating. The assessment resulted in 13 new recommendations, as well as a determination that 9 of 26 recommendations from previous FISMA audits remained open as of FY 2021.

Initial Performance Summary

United States Agency for International Development (USAID)

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
Protect	Managing Risk	Managed and Measurable
Detect	Managing Risk	Managed and Measurable
Respond	Managing Risk	Managed and Measurable
Recover		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	1	1
E-mail	6	2	10
External/Removable Media	3	1	2
Impersonation	0	0	0
Improper Usage	22	37	30
Loss or Theft of Equipment	3	3	0
Web	24	46	14
Other	103	65	60
Multiple Attack Vectors	1	2	2
Total	**162**	**157**	**119**

CIO Self-Assessment

The USG experienced multiple data breaches and compromises from the nation's strongest adversaries, resulting in numerous government actions and Emergency Directives (EDs). Agencies must actively work to recover from these recent attacks and stay ahead of this adversarial landscape. These types of attacks are complex and could quickly outpace an agency's ability to respond. The Agency's global workforce is the first line of defense in securing the Agency's data, including PII. The Agency's improved workforce education with an expanded awareness campaign, issuing numerous Cybersecurity and Privacy notices and alerts. The Agency's also expanded its Anti-Phishing program, focusing attention on this primary cyber threat to The Agency, by sending targeted imitation phishing emails using real-world scenarios to train staff to spot phishing attempts. To strengthen The Agency's cybersecurity posture and continue to reduce its attack surface and exposure from threat actors, the Agency responded to 4 EDs and 2 Binding Operational Directives (BODs) by mitigating the underlying risks as prescribed by DHS CISA. The Agency's cyber workforce continued to employ advanced cybersecurity tools to detect and mitigate malware attacks, phishing emails, and unauthorized data exfiltration, including threats to PII and Advanced Persistent Threats. The Agency's was able to mitigate and reduce cybersecurity risks to the Agency's network, data, and protect its workforce while continuing to deliver on its mission in more than 80 countries around the world.

Independent Assessment

USAID's information security program was evaluated as part of the FY 2021 FISMA Audit, which was conducted by CliftonLarsonAllen LLP (CLA). This audit included an evaluation of a sample of 6 of 52 USAID internal and external information systems in USAID's FISMA inventory as of February 12, 2021. The FY 2021 FISMA Audit noted that USAID implemented an effective information security program and practices by achieving an overall Managed and Measurable maturity level based on the FY 2021 IG FISMA Reporting Metrics. There were a few recommendations made to help USAID improve their information security program. These recommendations can be found in the FY 2021 FISMA Audit report.

Initial Performance Summary

Department of Agriculture

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	1	1	8
E-mail	22	3	11
External/Removable Media	0	0	6
Impersonation	0	1	0
Improper Usage	223	132	74
Loss or Theft of Equipment	4	7	25
Web	157	14	14
Other	227	149	507
Multiple Attack Vectors	13	1	1
Total	**647**	**308**	**646**

CIO Self-Assessment

FY21 was the first year in which all information security continuous monitoring capabilities were executed at the Departmental and Mission Area levels. After the Security Operation Center consolidation in FY 2020, a majority of the security capabilities were implemented successfully. USDA's Information Security Program maintained a grade of C in the Cyber category of the Federal Information Technology Acquisition Reform Act Dashboard, which reflects improvements in many parts of the program

The Inspectors General annual assessment indicates that USDA maintained an overall maturity rating of Consistently Implemented and raised the maturity of the Cybersecurity Framework function Detect from Defined to Consistently Implemented. Three ratings improved at the Domain level; Risk Management matured from Ad Hoc to Consistently Implemented, Data Protection and Privacy matured from Ad Hoc to Defined, and Information Security Continuous Monitoring matured from Defined to Consistently Implemented.

Implemented as a proof of concept, the RMF 2.0 activities, processes, and information needed to establish and maintain the security controls necessary for the resilience and survivability of information systems.

Established a strategy and road map for an enterprise-wide Technology Zero Trust Architecture, in compliance with the Executive Order 14028 on Improving the Nation's Cybersecurity.

In accordance with Binding Operational Directive 20-01: Develop and Publish a Vulnerability Disclosure Policy,

Independent Assessment

The Department took some positive steps for improving its security posture in FY 2021. For example, the Department issued several revised Departmental Regulations (DRs) and Departmental Manuals (DMs). The Department continued to centralize and consolidate operations. In general, we found the Department's security program was inconsistently implemented over the entire Department. Improvements are still needed for all the five functions. While the Department continued to centralize and consolidate operations the Department's senior management needs to continue its efforts to centralize and manage common functions at the Departmental level. It is more efficient and effective to control, monitor, evaluate, and react to centrally managed controls than allow individual agencies to manage these control activities. In brief, there are still many areas that the Department did not have the necessary assessment and enforcement processes in place to ensure agency compliance.

published a formal Vulnerability Disclosure Policy implemented the process researchers can take to find and report vulnerabilities in a legally authorized manner

Matured Security Operation Center activities to improve the progression of incidents from investigation through mitigation. Updated the Cyber Incident Response Playbook to enhance the incident response processes and outcomes.

Initial Performance Summary

U.S. Trade and Development Agency

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
Protect	Managing Risk	Optimized
Detect	Managing Risk	Ad Hoc
Respond	Managing Risk	Consistently Implemented
Recover		Optimized
Overall	**Managing Risk**	

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	0	3
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**3**

CIO Self-Assessment

USTDA has in the last fiscal year to continuously improve and enhance the security of our information services. USTDA is finalizing it's FY 2021 initiatives including the rollout of Microsoft Enterprise level solutions, SharePoint online, and Intune. These improvements, as well as the implementation of a Network Attached Storage (NAS) solution in FY 2021, provide enhanced security and capabilities to include greater network storage for end-user data and capacity for future growth. The implementation of CISCO DUO two-factor authentication and a Freedom of Information Act solution FOIAXpress, enabled the Agency to cloud-based solutions adhering to the new Cloud Smart strategy in accordance with Executive Order 13800. In FY 2022 USTDA will continue its FY 2021 initiative to fully implement SharePoint online to leverage more automation, enhance document management capabilities and implement tools for external collaboration . FY 2022 initiatives also include implementing LogicMonitor a cloud-based infrastructure monitoring that will allow USTDA to identify network and server issues early and assist in optimizing the overall IT environment. Likewise, USTDA plans to enhance the agency's security posture by participating in the Continuous Diagnostics & Mitigation (CDM) shared services in accordance with Executive Order 14028.

Independent Assessment

Cyberscope calculations would calculate as Optimized because 3 out of 5 categories are optimized. However, there are quantitative and qualitative measures missing min each of the functions/domains and Privacy and ISCM is AdHoc. As such adjusted to MM.

Controls not meeting Managed and Measurable:

IDENTIFY (NIST 800-53 controls): IGM6 Info Sec Arch; IGM8, 9 Metrics. IGM10 Automated risk solution; IGM12-16 SCRM

PROTECT (NIST 800-53 controls): IGM18, 23, 24, 37, 43 Metrics; IGM35, 36, 38, 39 Privacy; IGM42 SAT tailoring

DETECT (NIST 800-53 controls): IGM47-50 ISCM defined processes and metrics.
RESPOND (controls covered in other areas): IGM52, 54, 54, 55, 56, 58 Metrics
RECOVER (controls covered in other areas): IGM 64 backup processes in ISCM processes; IGM65 Metrics

Initial Performance Summary

Department of Veterans Affairs

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

Incidents by Attack Vector	FY19	FY20	FY21
Attrition	0	0	0
E-mail	162	233	166
External/Removable Media	14	0	4
Impersonation	2	0	3
Improper Usage	13	21	104
Loss or Theft of Equipment	498	302	593
Web	89	7	211
Other	49	375	0
Multiple Attack Vectors	0	3	0
Total	**827**	**941**	**1,081**

CIO Self-Assessment

As COVID continually reshapes how VA works, VA staff have adapted to ensure continuity of care and operations for our Veterans. This involved working with staff and accommodating their unique situations during COVID, allowing them to work remotely when possible and ensuring a safe workspace for those who could not. As the human element shifted, VA also introduced new technologies to allow for a remote work environment that could handle the work and security demands of our workforce and the Veterans who rely on it. Finally, VA strengthened relationships with other government agencies and vendors providing the necessary information and equipment to ensure continued operations. Providing alternate Personal Identity Verification (PIV) capabilities for telework and promoting cybersecurity and privacy awareness have been key to ensuring safe and secure continuity of operations. PIV cards are a central security measure at VA, acting as an ID badge for both entrance to facilities and access to the network. As COVID-19 remains a concern, it continues to be difficult and often impossible for staff to get to VA facilities to update their PIV cards, severely limiting their ability to telework. To combat this, VA developed an alternative (alt) card. Using MyDigitalID Remote Certificate Renewal, a digital tool, VA staff could apply for a temporary alt card. This process provided an alternative security method for VA employees, allowing staff to continue providing services to Veterans. Additionally, VA hosted a weeklong cybersecurity and privacy awareness event called Information Security and Privacy Awareness Week (ISPAW). This event focused on telework and secure home office best practices, improving staff's cybersecurity and privacy awareness knowledge to improve their individual security posture–and ultimately, VA's. VA also introduced new technologies allowing for safe and secure remote access to VA's network.

Independent Assessment

VA has made strides and implemented comprehensive security controls in many areas including enhanced monitoring of network traffic, scanning and patching of devices, and standardization of security control functions. However, VA still faces many challenges when it comes to consistently applying effective controls to its entire inventory of systems. Many issues continue to be identified related to significant risk areas such as access and configuration management on some systems while others are receiving more attention/resources. Additionally, VA is not consistently or completely addressing all aspects of the Risk Management Framework for its entire system portfolio. Due to the issues we identified throughout the audit cycle, we have assessed the VA's overall information security program to be ineffective.