FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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

A distributed workforce teleworking during COVID-19 required changes to the telework and access model. The Advisory Council on Historic Preservation (ACHP) had been preparing before the emergency with Zero Trust access models and was able to rapidly deploy remote access securely. In preparation for a longer environment with the new operating model, the agency is implementing additional security controls through micro-segmentation, continuous vulnerability and security instrumentation testing, and security orchestration and automation.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Advisory Council on Historic Preservation was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Section 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

African Development Foundation

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

Incidents by Attack Vector	FY18	FY19	FY20
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 United States African Development Foundation (USADF) has developed a Governance Risk and Compliance (GRC) strategy through the implementation of a risk management structure that addresses the organization-wide risk. The USADF's leadership strives to mitigate cybersecurity risks by enforcing an organization-wide enterprise risk management plan, active participation in the DHS' CDM program and monthly security assessments to address evolving cyber threats. The USADF performs an annual security assessment and authorization on its information system resources according to the NIST SP guidelines and in compliance with the Federal Information Security Modernization Act of 2014. The USADF enforces layers of cybersecurity protection by leveraging FedRAMP approved advanced cloud technologies and US government shared services. The USADF has implemented the mandated DHS EINSTEIN 3A IPSS DNS and IPSS Cloud Email as part of its effort to mitigate and reduce cybersecurity risk exposure.

Prior to COVID-19, USADF engaged into a cloud-based strategy migrating IT resources to the cloud and implementing an Identity ICAM solution with OKTA, which mitigates cybersecurity threats through enhanced access controls and implementation of multi-factor authentication. Access to all Government Shared Services are through secure remote access and VPN technologies which are monitored and logged. Implementing these cybersecurity measures and developing a mitigation strategy made transitioning to remote/telework operation during COVID-19 less challenging for USADF.

USADF completed a full security assessment and authorization for 2020 that reviewed all security controls for its GSS based on NIST requirements.

Independent Assessment

USADF's information security program was evaluated as part of the FY 2020 FISMA Audit. For this audit, CLA reviewed selected controls related to the FY 2020 IG FISMA Reporting Metrics from 3 of 9 information systems in USADF's systems inventory as of May 2020. The FY 2020 FISMA Audit noted 72 of 76 selected NIST SP 800-53, Revision 4 security controls were properly implemented. This along with the maturity of USADF's information security program led to the determination of USADF having an overall effective information security program. There were a few recommendations made to help USADF improve their information security program. These recommendations can be found in the FY 2020 FISMA Audit report.

FY2020 Annual Cybersecurity 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	Consistently Implemented
Respond	At Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	1	3
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	1	5	4
Multiple Attack Vectors	0	0	0
Total	**3**	**6**	**7**

CIO Self-Assessment

The American Battle Monuments Commission (ABMC) has identified the vulnerabilities and recognized the potential risks of its legacy on-premise systems. The Agency has started migrating to a new full cloud IT Infrastructure in FY 2020, with expected completion in Q2 FY 2021. In the context of increased telework, the Agency was successful in mitigating associated risks by onboarding Unified Communication tools such as Microsoft Teams and leveraging Secure Access Service Edge (SASE) to phase out legacy VPN access. The Agency has deployed TIC 3.0 tools, processes and procedures to meet contingency and security objectives.

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 as an organization has historically lacked documentation of policies and procedures. This known issue has created many of the results noted in our FISMA evaluation. This issue has been and is being aggressively addressed by ABMC management.

ABMC has identified a multitude of POA&M to address identified FISMA issues, and ABMC has made addressing FISMA requirements one of their highest priorities in the organization. This can be evidenced by the addition of a full-time CISO in FY 2020.

ABMC has an information security program that continues to mature, and will further mature with their modernization efforts put in place in FY 2020 and being implemented in FY 2021.

ABMC's information security program can further mature in the following areas:

- Data protection and privacy
- Information security continuous monitoring
- Contingency planning

The scope of this evaluation covered ABMC agency-owned and contractor-operated information systems of record as of September 30, 2020.

FY2020 Annual Cybersecurity Performance Summary

Armed Forces Retirement Home

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

Incidents by Attack Vector	FY18	FY19	FY20
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 Armed Forces Retirement Home's (AFRH) 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.

AFRH, in coordination with the Department of Interior Office of the Chief Information Officer 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 to:

- Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or information systems; and
- 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

AFRH conducts an annual risk assessment to identify security weaknesses which consists of technical testing, interviews and observation techniques. The assessor analyzed 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 of data hosted by the system as described in the AFRH system security plan. 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.

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

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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

Prior to COVID-19, all 3 Barry Goldwater Scholarship Foundation employees were already telework capable with security measures in place. The transition to 100% telework only increased the frequency of telework.

Independent Assessment

The Barry Goldwater Foundation is a small agency with two permanent employees and limited resources. The agency coordinates with our federal agency service providers, contracted IT support, and the website/program coordinator, regularly regarding operating systems and security.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	1	0	1
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	1	1
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	1	2	5
Multiple Attack Vectors	0	0	0
Total	**2**	**3**	**7**

CIO Self-Assessment

The FRB took many steps to secure the virtual telework posture. To ensure the FRB’s security posture was not degraded due to the 100% remote work status, the FRB tuned and tested its continuous monitoring tools and processes in order to verify they were equally effective in the full remote state as when staff were in the office. In order to support FRB staff whose PIV cards expired and were unable to be renewed due to the pandemic, the FRB implemented a secure alternative method for local and network user authentication. To support secure collaboration, the FRB implemented alternative secure tools to support video conferencing and other collaboration needs. In addition, the FRB developed guidance to assist staff is securely participating in video conference meetings hosted by external parties.
Beyond the move to a 100% remote work posture, the primary cyber security risks that impacted the Board in 2020 include phishing emails carrying advanced malware; ransomware; and distributed denial-of-service (DDOS) attacks that target the availability of data and systems; vendor risks, including an increased use of cloud services; and trusted insiders with access to sensitive data. The Board’s cyber risk governance program is built upon the principles of defense-in-depth and continuous improvement. Key enhancements in 2020 included strengthening our monitoring capabilities; enhancing vendor risk management processes; continuing to partner with DHS to implement the Continuous Diagnostic and Mitigation (CDM) program at the Board; and implementing enhanced user behavior monitoring processes. In addition, we conduct 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; perform red and purple team tests; and have independent third-party assessments performed beyond the work done by the Office of Inspector General.

Independent Assessment

Overall, we found that the Board continues to maintain an effective information security program. We also found that the Board's information security program includes policies and procedures that are generally consistent with the functional areas outlined in the NIST Cybersecurity Framework. However, we identified opportunities to strengthen processes and controls in the areas of risk management, configuration management, identity and access management, data protection and privacy, and ISCM to further mature the program and ensure that it remains effective. Our audit report includes four recommendations and two matters for management's consideration to strengthen controls in these areas.

FY2020 Annual Cybersecurity Performance Summary

Chemical Safety Board

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	FY18	FY19	FY20
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 Chemical Safety Board's cybersecurity posture has not changed dramatically due to the expansion of telework under the COVID-19 national emergency. The agency already has in place many of the requirements of telework, given the nature of the agency's mission and its already dispersed workforce. With a small number of employees (34 at present) divided between Headquarters in Washington and the Western Regional Office in the Denver Federal Center, our employees are accustomed to working from the road when deployed and working from home as well. Our small infrastructure has long supported remote connections via Cisco VPN remote access and access between HQ and the WRO over a LAN-to-LAN tunnel, all of which appears to the user as one local area network. Remote administration, continuous monitoring, encryption, and antivirus/malware protection and management have proceeded as usual during the pandemic.

Independent Assessment

This matrix was completed by an independent assessor that performed the work as directed under contract with the EPA's OIG.

The U.S. Chemical Safety and Hazard Board's Information Security Program continues to mature. During the FISMA Assessment concerns were identified related to Risk Management, Flaw Remediation, Training, Disaster Recovery Testing and maintaining back-ups at an alternate location. The concerns related to Disaster Recovery Testing and maintaining back-ups at an alternate location are areas where the design of procedures was adequate how the related operating processes had been discontinued as a direct result of COV-19 protocols. Recommendations have been made to enhance the control environment in areas where concerns were identified. The overall design of the Information Security Program has been concluded as effective, procedures in place are adequate and situate this agency for continue growth in the maturity of these processes.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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 primary effort to improve security posture was award for updated telecommunications services, including MTIPS, Managed Network Services and Managed LAN services under the GSA administered EIS contract. Award of this contract marks the beginning of moving away from outdated services under expiring contracts.

Like all agencies, the necessity of remote working due to the COVID-19 national emergency posed significant challenges to the Commission of Fine Arts (CFA). Prior to 2020, telework was not performed on a regular basis and therefore, remote work infrastructure was not in place. The CFA's internal network resources are not, and never have been, accessible from outside its physical plant; so somewhat ironically, the internal network is possibly more secure during the pandemic. In the absence of access to the internal network, the CFA availed itself of reputable third-party file sharing solutions and began taking steps to upgrade its existing cloud service to a more advanced solution. The majority of staff was issued GFE (i.e., laptops), and overall agency operations saw little adverse impact. The most significant identified cybersecurity risk, perhaps highlighted by the pandemic crisis, 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

An independent evaluation of the status of the IT cybersecurity program for the Commission of Fine Arts was not performed for FY 2020, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Section 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

Commission on Civil Rights

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	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
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 United States Commission on Civil Rights (USCCR) relies extensively on IT resources to accomplish its mission. The overall FY 2020 FISMA maturity score for USCCR's security program is Consistently Implemented. The USCCR maturity score for FY 2019 was also Consistently Implemented. 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 DHS BODs and EDs. 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.

Despite 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 modern and secure Operating System (OS) to move past the unsupported OS endpoints. As a result, USCRR hopes to continue the IT Modernization Plan in FY 2021 to increase its maturity.

Independent Assessment

The United States Commission on Civil Rights (USCCR) relies extensively on IT resources to accomplish its mission. The overall FY 2020 FISMA maturity score for USCCR's security program is Consistently Implemented. The USCCR maturity score for FY 2019 was also Consistently Implemented. 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 DHS BODs and EDs. 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. Despite 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 modern and secure Operating System (OS) to move past the unsupported OS endpoints. As a result, USCRR hopes to continue the IT Modernization Plan in FY 2021 to increase its maturity.

FY2020 Annual Cybersecurity 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	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	0	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	2	1
Web	0	0	0
Other	2	2	1
Multiple Attack Vectors	0	0	0
Total	**3**	**4**	**3**

CIO Self-Assessment

The risk landscape and external influences are changing - COVID-19 has presented new challenges. The Commodity Futures Trading Commission (CFTC)'s cybersecurity program is built to address the growing threat landscape, with a balanced mix of policy and compliance activities that govern the protection of our data, assets and mission functions. Recently identified risks include weaknesses related to internal controls; specifically, implementing contingency plan improvements to lower the risk of data loss, and strengthen security controls for the CFTC's cloud presence. We revisited our high value data designation during FY 2020. Identifying, protecting and securing high value data and mission essential functions require capabilities and resources that are currently not in place, including a mature Insider Threat Program, and automated tools with predictive and preventative technologies. Key gaps that have been identified in our information security program include:

- Fulfill DHS CDM program dependencies;
- Timely remediation of POA&M on major systems;
- Develop role-based security training for FISMA mandatory roles;
- Develop an insider threat program to include data loss protection (DLP) capability;
- Maintain a safe and secure telework operating environment during the pandemic by leveraging the Interim Telework Guidance published by CISA. Provide alternate multi-factor authentication method to validate remote users; and
- Improve ability to perform agent-based vulnerability scans and patch remote GFE.

The impacts of added requirements from the cybersecurity legislation, our understanding of the current threat landscape, and the constant evolving practices of cybersecurity, 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 provide information assurance and computer network defense for our mission critical systems and data.

Independent Assessment

For the reporting period, we rated CFTC's IT security program as "Effective" using CIGIE's and DHS's maturity evaluation tool.

We recommended that CFTC management (ODT and Privacy Office):

- ODT take action on FY 2020 AD Program and Backup and Recovery controls findings and consider process improvement opportunities to further enhance the agency's mission to protect trader data and personal and identifiable information.

AD Program Review: We tested the program's configuration settings and concluded that 78 of 93 configuration settings align with the vast majority of NIST controls and industry best practices. It was also noted that one failed control posed a low-to-moderate risk to the CFTC domain. In addition, 14 configuration settings should be reviewed as Process Improvement Opportunity (PIOs) opportunities that were not required but deemed as best practices. We recommend that ODT remediate the one failed control and review the PIOs identified for possible enhancements to the CFTC's Active Directory program.

Backup and Recovery IT controls assessment: We evaluated process controls settings and concluded that 15 of 16 process control settings align with the majority of NIST controls and industry best practices. It was also noted that one failed control posed a low-to-moderate risk to the CFTC domain. In addition, six process controls settings should be reviewed as Process Improvement Opportunity (PIOs) opportunities that were not required but deemed best practices. We recommend that ODT remediate the one failed process control and review the PIOs identified for possible enhancements to the CFTC's backup and recovery process.

Privacy Office: Take action on two FY 2020 Privacy Program findings and coordinate with OGC to develop guidance to coordinate parade with business partners to meet federal mandates on Privacy Law requirements.

FY2020 Annual Cybersecurity Performance Summary

Consumer Financial Protection Bureau

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	3	3	0
Loss or Theft of Equipment	151	100	57
Web	0	0	0
Other	10	0	7
Multiple Attack Vectors	0	1	0
Total	**164**	**104**	**64**

CIO Self-Assessment

Since established, the Consumer Financial Protection Bureau (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 become 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;
- 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; Safeguarding sensitive information from misuse, while also making the appropriate data available to carry out CFPB's mission.

In 2020, CFPB has taken measure to mitigate risks due to the COVID-19 national emergency. CFPB established a Teleconference Participation Directive that provides uniform guidance on CFPB user conduct when participating in teleconferences or virtual meetings hosted through CFPB authorized and unauthorized platforms. The Cybersecurity team conducts analysis of COVID-19 themed cyber threat activity daily, subscribes to multiple threat intelligence resources including DHS, and tailors the cybersecurity awareness communications. Additionally, the CSIRT provides daily reports on COVID-19 threat activity to senior leadership.

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 risk management 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 configuration management to ensure that its information security program remains effective. Our FY 2020 FISMA audit report includes 1 recommendation to strengthen controls in this area.

FY2020 Annual Cybersecurity Performance Summary

Consumer Product Safety Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	3	3
Loss or Theft of Equipment	5	1	0
Web	0	0	0
Other	2	1	2
Multiple Attack Vectors	0	0	0
Total	**8**	**5**	**5**

CIO Self-Assessment

The Consumer Product Safety Commission's (CPSC) IT security priorities identified at the beginning of FY 2020 included focusing on:

1. Enhancing the POA&M process;
2. Implementation of technology to support privileged access management;
3. Enhancing the agency privacy program;
4. Implementing enhanced malicious activity detection capabilities; and
5. Improving patch management.

During the year, the Agency increased focus on POA&M activities and enhanced POA&M tracking and reporting. This resulted in the continual trend of reducing open POA&Ms across all major agency information systems. The Agency completed its implementation of an enterprise-wide privileged access management system. The Agency hired a privacy officer to manage the Agency's privacy program. The Agency deployed security tools to help provide greater awareness of potential malicious activity affecting agency information systems. The Agency also implemented the CDM Phase I tools to enhance visibility into the Agency's security posture. The Agency implemented an automated patch management system to help increase timely patch deployment.

Independent Assessment

We evaluated CPSC's information security program's policies, procedures, and practices as a whole and tested the effectiveness of CPSC 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 15 recommendations included in the FY 2019 FISMA report, and the CPSC has:

- Continued development of a formal Enterprise Architecture (EA);
- Made progress on completing POA&Ms;
- Continued the implementation of technology to support privileged user account management;
- Hired an additional person to support the privacy program;
- Continued the implementation of Information Security Continuous Monitoring (ISCM) program system level requirements;
- Further enhanced network defenses by baselining network activity through the use of network profiling techniques; and
- Performed some business impact analysis tasks to enhance contingency planning.

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.

FY2020 Annual Cybersecurity Performance Summary

Corporation for National and Community Service

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	3	5
Loss or Theft of Equipment	1	0	2
Web	0	0	0
Other	0	3	5
Multiple Attack Vectors	0	0	0
Total	**2**	**6**	**12**

CIO Self-Assessment

AmeriCorps (formally the Corporation for National and Community Service (CNCS) has endured some security risk during the COVID-19 pandemic, and the organization has taken a series of actions. Prior to the beginning of the COVID-19, AmeriCorps tested full scale telework program verifying user functionality and systems environment capabilities. At the completion of the test, we discovered two technical issues: poor bandwidth and PIV authentication access. AmeriCorps network bandwidth was inadequate causing severe Internet latency, poor video, and VPN interruptions. The organization sought immediate resolution by upgrading our bandwidth from a 100 megabyte to a 1 gigabyte.

Regarding PIV for authentication, AmeriCorps relaxed PIV enforcement policy for new users, and employees with damaged or unusable cards as replacement card locations were not operational as part of the COVID-19 response.

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 enforced multi-factor authentication across the enterprise. This helped reduce the risk in the identify function area by reducing the use of username/password and increasing reliability of granting an authorized person access to information. AmeriCorps' cybersecurity program is on the right trajectory that will continue to protect vital information that helps us achieve our mission.

Independent Assessment

We have determined that CNCS's information security program is Not Effective, as the five FISMA security function areas in its information security program and practices have not achieved sufficient maturity. CNCS faces ongoing challenges in the consistent implementation of its information security program and the monitoring of security controls. There are continuing deficiencies related to organization-wide risk management, IT asset inventory management, configuration management, vulnerability management, identity and access management, mobile device management, data protection and privacy, and logging and monitoring practices designed to protect mission-critical systems. These gaps limit the protection of CNCS's systems and data and may expose sensitive information, including personally identifiable information, to unauthorized access and use.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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 Council of the Inspectors General on Integrity and Efficiency (CIGIE) has taken steps toward improving our security posture and reaching FISMA compliance. Our most significant achievements are as follows:

- CIGIE is currently working with a specialized contractor implementing HSPD-12.
- CIGIE has upgraded non-FISMA Wi-Fi infrastructure to incorporate FIPS 140-2 compliant only equipment.

- CIGIE has upgraded all network switches to FIPS 140-2 fully managed equipment.
- CIGIE has implemented a more advanced authentication of guest Wi-Fi devices.
- CIGIE has achieved account integration between cloud and on-premise AD achieving single sign-on.
- 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 mobile devices.
- CIGIE has enhanced its endpoint protection by deploying advanced threat protection (ATP) with centralized management capabilities.
- CIGIE has replaced its legacy domain controllers to modern servers.
- CIGIE has implemented a centralized monitoring server with advanced detection capabilities.
- CIGIE has implemented DLP capabilities in our cloud tenancy.
- CIGIE has implemented a technology that allows us to update in-use and not in-use laptops, ensuring that all are patched regularly.
- CIGIE has reviewed and further locked down internal SMTP relay servers.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Council of the Inspectors General on Integrity and Efficiency was not performed for FY 2020, and the IG assessment section is marked “Not Applicable.” Per FISMA, Section 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity 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	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
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	1	0	0
Web	0	0	0
Other	1	2	0
Multiple Attack Vectors	0	0	0
Total	**5**	**3**	**0**

CIO Self-Assessment

Cybersecurity continues to be one of the Agency's top priorities. In accordance with OMB and DHS 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 COVID-19 national emergency, 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 FY 2020, the Department of Justice OIG reviewed the information security program for 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 4 - Managed and Measurable" 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 two Security Function areas of Identify and Protect. The Agency should implement our recommendations specifically within the Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training metrics of the Identify and Protect Functions to improve the effectiveness of the Agency's information security program.

FY2020 Annual Cybersecurity Performance Summary

Defense Nuclear Facilities Safety Board

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

Incidents by Attack Vector	FY18	FY19	FY20
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	2	3	1
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	**2**	**4**	**1**

CIO Self-Assessment

The Defense Nuclear Facilities Safety Board (DNFSB) has made progress towards the cybersecurity risks of the general support system (GSS) during FY 2020. Current DNFSB cybersecurity risks include hardware and software asset protection and detection, security training and protection, and system configuration. During FY 2020, DNFSB purchased and is implementing a solution regarding protection and detection for the software and hardware assets. Additionally, DNFSB worked to purchase a cloud service to mitigate the risk areas of security training and protection. Finally, DNFSB is taking steps towards removal of the vulnerabilities caused by outdated system configurations with the installation of a modern operating system.

Independent Assessment

DNFSB continues to address the gaps identified in a 3rd-party risk assessment performed in FY 2019. DNFSB has a good plan and direction. Due to the small organizational structure, DNFSB can operate and communicate more efficiently and effectively compared to larger Federal agencies. DNFSB's key risk management personnel are intimately involved in all aspects of DNFSB's information security program and are aware of every important decision involving risk to the Agency's information system, information, and mission. 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 DNFSB's information system, information, and missions.

FY2020 Annual Cybersecurity Performance Summary

Denali Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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 greatest cybersecurity risks Denali Commission faces are social engineering-related attempts from foreign and domestic sources --phishing and other scams intended to obtain credentials and access to agency resources, which may be used as gateway access for Advanced Persistent Threat (APT) operations. Application of BOD 18-01 to Denali systems, employee education and judicious application of least privilege principles are the primary defenses against this threat. Generic risk of compromise via vulnerability or exploit always exists. Denali Commission has worked with federal cyber-liaison resources to remediate issues defined via Emergency Directives, BODs, and scans. Patching for Denali Commission is performed on schedules compliant with directives and requirements. Denali Commission is following its existing remote access protocol in place prior to the pandemic for COVID-19 telework. The Denali technology service provider is not aware of any special provisions. Denali Commission has worked to improve its cybersecurity policies and procedures to advance its maturity stance throughout the year.

Independent Assessment

The Denali Commission's information security program was deemed ineffective because of clear delineation, communication and documentation of the roles and responsibilities at the organizational and information system levels for stakeholders involved in information security and configuration. The Commission has hired a contractor to assist in its efforts to continue work on documenting and putting the appropriate policies and procedures in place and to ensure that the technology and tools in place are fully utilized for maximum effectiveness.

FY2020 Annual Cybersecurity Performance Summary

Department of Agriculture

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	1	1	1
E-mail	20	22	3
External/Removable Media	1	0	0
Impersonation	0	0	1
Improper Usage	323	223	132
Loss or Theft of Equipment	9	4	7
Web	161	157	14
Other	365	227	149
Multiple Attack Vectors	49	13	1
Total	**929**	**647**	**308**

CIO Self-Assessment

In FY 2020, the United States Department of Agriculture (USDA) concluded the consolidation of its security operations that was started in FY 2018. Over that time USDA consolidated software and hardware tools, unified disparate processes, and realigned 128 personnel. In FY 2020, the Department increased its overall cybersecurity maturity level to Level 3, “Consistently Implemented,” by maintaining or improving 90% of the OIG metrics. The Department also achieved a grade of C in in the Cyber category of the FITARA Dashboard reflecting a full letter grade improvement based on progress in the Inspectors General assessment and the cross-agency priority cybersecurity goals.

To address the risks resulting from the expansion of telework, the Department expanded its remote access capabilities for voice and data to handle the increased telecommunications needs and modified its vulnerability scanning and patching capabilities to ensure remote systems are compliant with the most current cybersecurity requirements. Additional risks resulted from delays from maintaining or obtaining current PIV credentials to access Departmental systems. A surge in hiring for the fire season impacted the ability to manage those accounts dynamically.

The challenge for USDA’s cybersecurity program is to mature its cybersecurity practices across all Mission Areas and five functions of the Cybersecurity Framework. Four cybersecurity priorities for FY 2021 are:

1. Address outstanding audit recommendations.
2. Improve its continuous diagnostic and monitoring capabilities and practices.
3. Improve the cybersecurity of HVAs.
4. Improve vulnerability management focusing on patch and system upgrade processes.

Each of the priorities will build on efforts that have already started and will take advantage of additional tools, and centralized practices, and enterprise-level oversight.

Independent Assessment

The Department took some positive steps for improving its security posture in FY 2020. For example, the Department issued several revised Departmental Regulations (DR) and Departmental Manuals (DM). Although not released, it continues to review and update the DRs and DMs during FY 2020. The Department continued to centralize and consolidate operations. In general, we found the Department security program was inconsistently implemented over the entire Department. Improvements are still needed for many functions. While the Department implemented a tracking tool, to aid in governance, we found a lack of oversight detracted from its use as a management tool. In brief, there are still areas that the Department did not have the necessary assessment and enforcement processes in place to ensure agency compliance.

FY2020 Annual Cybersecurity Performance Summary

Department of Commerce

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	FY18	FY19	FY20
Attrition	4	14	3
E-mail	660	330	402
External/Removable Media	0	0	0
Impersonation	2	2	6
Improper Usage	582	722	851
Loss or Theft of Equipment	67	29	38
Web	196	59	114
Other	305	284	276
Multiple Attack Vectors	11	23	33
Total	**1,827**	**1,463**	**1,723**

CIO Self-Assessment

In FY2020, the Department of Commerce (DOC) continued to face the same primary IT security risks as in recent years: lack of near-real time continuous monitoring to facilitate standardized risk-based IT security management, including the ability to monitor the implementation of NIST SP 800-53 controls across all of DOC, challenges implementing enhanced security requirements across HVA systems, and deficiencies in the timely identification and mitigation of vulnerabilities.

DOC also encountered new risks due to COVID-19 related mandatory telework, including challenges with active scanning and monitoring of IT resources used to support telework and challenges issuing new PIV credentials and ensuring the maintenance of PIV certificates. To mitigate these risks, the DOC continued its integration of the Enterprise Security Operations Center and Enterprise Continuous Monitoring Operations programs to fortify DOC endpoints and facilitate the core capability for the CDM program to address Hardware Assets Management, Configuration Management, and Vulnerability Management capabilities.

DOC continued to implement its enterprise IT Security Baseline Policy, which was released in FY 2019 and enhances security requirements to strengthen the DOC's IT Security posture. DOC has continued the use of an anti-phishing exercise tool to train employees on the attributes of phishing attacks. DOC continued to improve the implementation of enhanced security controls on HVA systems, and instituted a repeatable, data-driven approach to identify HVAs, applying an HVA Identification Tool to every DOC FISMA-reportable system. DHS conducted Risk and Vulnerability Assessments for two DOC HVAs, and a Security Architecture Review assessment for one DOC HVA.

To mitigate risks presented by being unable to issue and maintain PIV credentials, DOC used alternate two-factor authentication methods such as RSA tokens and worked with GSA on a process to allow the renewal of certificates on the credential before they expire

Independent Assessment

The Department of Commerce (DOC), OIG completed an audit of the Department's information security program. OIG reviewed a representative subset of 12 IT systems across DOC and its bureaus. OIG assessed each of the five functional areas (Identify, Protect, Detect, Respond, and Recover) and found all were a maturity level 2. While DOC defined policies and procedures, it did not consistently implement those policies and procedures across the selected systems. As a result, DOCs information security program has scored an overall maturity rating of level 2 (defined) and is therefore not fully effective.

FY2020 Annual Cybersecurity Performance Summary

Department of Defense

CIO Self-Assessment

The Department of Defense (DoD) uses several cyber scorecards to assess and respond to a constantly evolving risk posture. The COVID-19 pandemic added an additional input to that risk calculus, as it required the Department to continue to execute its national security mission with a massively expanded remote workforce on short notice. To mitigate this cybersecurity risk, the DoD CIO stood up the COVID-19 Telework Readiness Task Force in March. Key task force efforts included expanding virtual private network capacity, issuing government-furnished mobile devices to conduct unclassified and classified teleworking, expanding secure video conferencing services, and introducing the Commercial Virtual Remote (CVR) environment. The CVR Environment is a DoD-contracted Microsoft Office 365 (O365) Teams capability implemented with DoD specific security controls which provides video, voice, and text communication, as well as document sharing tools for Basic Controlled Unclassified Information. The CVR environment provided an exceptionally quick and enterprise-wide augmentation of DoD's existing collaboration tools. Additionally, DoD CIO produced a Top Telework Tools Playbook for DoD that served as a reference guide for enterprise-approved collaboration tools, and a list of more tools that received provisional authorization for more limited uses with additional approvals. Any additional telework capabilities required DoD-level approval. This approach mitigated the risk that would otherwise have been engendered by a multitude of component-level tools. To further mitigate risk DoD will transition from CVR to Defense Enterprise Office Solution (DEOS), which will be hosted in an impact level 5 environment. DoD also increased safe file sharing with the milDrive and DoD Secure Access File Exchange (SAFE), two cloud-based solutions that permit secure and convenient access to large files from diverse locations.

FY2020 Annual Cybersecurity Performance Summary

Department of Education

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	2	0	1
E-mail	39	0	1
External/Removable Media	0	0	0
Impersonation	0	0	1
Improper Usage	40	62	51
Loss or Theft of Equipment	2	0	0
Web	4	0	5
Other	0	17	0
Multiple Attack Vectors	0	0	0
Total	**87**	**79**	**59**

CIO Self-Assessment

During FY 2020, the Department of Education (Department) successfully transitioned 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. We increased communications to Department users to emphasize cyber vigilance as well as individual responsibilities for data protection and privacy while structuring simulated phishing exercises around the current threat landscape to keep Department employees educated and vigilant. As a result of these efforts, the Department has been able to continue its important mission without interruption.

Throughout this year, the Department implemented tools, processes, and protections to maximize the quality, security, and privacy of our information systems and continued to develop and implement uniform and consistent governance policies and standards to strengthen the Department’s cybersecurity by enhancing protections of its IT infrastructure, systems, and data. In FY 2020, the Department updated or created a number of standards and instructions focused on strengthening our cybersecurity risk management practices. The Department continued to mature our risk management processes by enhancing our CSF Risk Scorecard to support automated data capture for near-real time risk scoring and reporting. This has enabled us to make the CSF Risk Scorecard available to our stakeholder community daily. In June 2020, we again expanded our outreach and risk communications by disseminating monthly “State of IT” reports to the Department’s senior leaders. These executive level reports provide the Department’s senior leaders with a holistic view of their IT investments, services, and cybersecurity posture through comprehensive IT and cybersecurity trends, metrics, and key insights to prompt top-down engagement and actions.

Independent Assessment

Our objective was to determine whether the Department’s overall IT security programs and practices were effective as they relate to Federal information security requirements. To answer this objective, we rated the Departments performance in accordance with FY 2020 IG FISMA Reporting Metrics. Although the Department had several notable improvements in implementing its cybersecurity initiatives, its overall IT security programs and practices were not effective in all of the five security functions. We had findings in all eight metric domains, which included findings with the same or similar conditions identified in prior reports. We determined the Department’s programs were consistent with (1) Level 2 - Defined, which is considered not effective for five domains: Risk Management, Identity and Access Management, Data Protection and Privacy, Security Training, and Information Security Continuous Monitoring; and (2) Level 3 - Consistently Implemented, which is considered not effective for three domains: Configuration Management, Incident Response, and Contingency Planning. For FY 2020, the Department has improved on several individual metric scoring questions from FY 2019, especially in the areas of Risk Management, Incident Response and Contingency Planning. The Department also demonstrated improvement in its processes from FY 2019 within several metric areas.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	1	3	5
E-mail	79	111	103
External/Removable Media	0	1	1
Impersonation	0	0	0
Improper Usage	172	231	270
Loss or Theft of Equipment	191	157	119
Web	42	29	10
Other	161	287	215
Multiple Attack Vectors	1	1	4
Total	**647**	**820**	**727**

CIO Self-Assessment

The Secretary stresses cybersecurity as a top priority and leadership across DOE play an active role in shaping cybersecurity risk management and mitigation activities. DOE faces cyber threats from nation state actors, advanced persistent threats, and disruptive non-state actors. Successful attack 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; forging interagency and 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 developed amplification guidance to assist sites in maturing POA&M, Risk Management and System Inventory processes. DOE continues to collaborate with DHS and the 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. DOE’s mature IT infrastructure and support of remote work during steady state operations enabled DOE to quickly transition to expanded telework under the COVID-19 national emergency. In response to telework expansion and the potential for increased risk, DOE increased enterprise monitoring of the remote work tools & appliances and raised awareness of remote working cyber threats through the distribution of guidance and tips to the workforce.

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 national security systems. Specifically, we reviewed the Department's progress towards meeting the DHS/OMB FISMA metrics at selected sites to assess the effectiveness of information security policies, procedures, and practices. Additional sites were scheduled to be assessed in FY 2020; however, the assessments will be conducted at a later date due to the COVID-19 pandemic. Overall, the OIG determined the Department was generally effective in implementing a cybersecurity program. While improvements should continue to be made, we found that the Department had Consistently Implemented (Level 3) each the following functions: Identify; Protect; Detect; and Recover. We found that the Department had achieved a Managed and Measurable (Level 4) maturity level for the Respond function. Because of the non-homogeneous nature of the Department's population, it is likely 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. The rating for each of the metrics includes the results of both unclassified and national security system environments.

FY2020 Annual Cybersecurity 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	Consistently Implemented
Respond	At Risk	Consistently Implemented
Recover		Defined
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	14	19	23
E-mail	885	603	798
External/Removable Media	16	2	0
Impersonation	26	5	0
Improper Usage	3,588	4,674	3,493
Loss or Theft of Equipment	823	575	326
Web	1,263	609	91
Other	3,063	1,088	2,501
Multiple Attack Vectors	0	33	11
Total	**9,678**	**7,608**	**7,243**

CIO Self-Assessment

Since the start of the COVID-19 pandemic, the Department of Health and Human Services (HHS) has witnessed heightened cybersecurity threats to include Distributed Denial of Service (DDoS) attacks, malicious spam and phishing, increased ransomware attacks, and misinformation. In responding to cybersecurity threats, HHS directly supports: The HHS community, which includes HHS' operating divisions such as the Centers for Disease Control and Prevention (CDC), the Food and Drug Administration (FDA) and the National Institutes for Health (NIH), each of which plays a critical role in COVID-19 response; The federal healthcare community consisting of Defense Health Agency (DHA) and the Department of Veterans Affairs (VA), with which HHS shares critical information regarding cybersecurity threats and vulnerabilities; and the healthcare and public health (HPH) sector, which brings together private sector healthcare delivery professionals to share information about cybersecurity threats and best practices.

Since March, HHS: Increased IT infrastructure capacity to enable widespread and secure remote work; Initiated the immediate transition from HHS' Trusted Internet Connection (TIC) to a Managed Trusted Internet Protocol Service (MTIPS) solution to enhance HHS' security posture; Analyzed 16,822 reported spam messages, 401 of which were malicious and 40 of which triggered malicious site takedown requests; Identified and researched 30 coordinated cybersecurity threat campaigns; Collaborated with HHS Assistant Secretary for Preparedness and Response (ASPR), the FBI, and DHS to identify organizations critical to the COVID-19 response effort and develop options for enhanced cyber hygiene, threat detection and information sharing; and, evaluated newly registered COVID domains for malware and reported malicious COVID-19 sites for takedown, as many as 67% of the reported domains were observed to be malicious.

Independent Assessment

Overall, while HHS was evaluated at the same level in FY20 and FY19 across the function domains, HHS continues to implement changes to strengthen the maturity of its enterprisewide cybersecurity program. However, it was determined that the HHS' information security program was 'Not Effective'. This determination was made based on (1) HHS not meeting a 'Managed and Measurable' maturity level for Identify, Protect, Detect, Respond, and Recover functional areas, (2) deficiencies identified within the Identify, Protect, and Respond functional areas, and (3) the evaluation of a maturity level below consistently implemented for some FISMA metric questions both at HHS overall and at selected operating divisions (OpDivs). Progress continues to be made to sustain cybersecurity maturity across all FISMA domains. Also notable were increased maturation of data protection and privacy and information systems continuous monitoring. The FY20 FISMA audit reflects the assessment of 5 of the 12 OpDivs and not the entire agency. HHS is a federated environment which brings challenges in attaining an effective program at all OpDivs. HHS is cognizant of opportunities which arise to strengthen the overall information security program which help ensure that policies and procedures in place at all OpDivs are consistently implemented and in line with the requirements across their security program. HHS continues to work towards implementing a Department-wide CDM program in coordination with DHS. The combination of HHS federated environment and separate funding streams has caused a variance in maturity and progress at each OpDiv. HHS should work with all OpDivs and system owners to consistently implement the established contingency planning program. HHS should also define risk-based metrics to measure the effectiveness of their information security program. These steps will help HHS achieve its mission through an effective and coordinated information security program.

FY2020 Annual Cybersecurity Performance Summary

Department of Homeland Security

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	1	1
E-mail	477	93	311
External/Removable Media	9	10	17
Impersonation	0	0	0
Improper Usage	143	544	121
Loss or Theft of Equipment	14	15	10
Web	64	30	41
Other	420	379	204
Multiple Attack Vectors	0	0	0
Total	**1,127**	**1,072**	**705**

CIO Self-Assessment

The DHS CIO non-concurs with the OIG’s overall assessment that
DHS regressed in the management of its information security program. Despite numerous meetings with Department and Component Program Officials, and subject matter experts, and the extensive supporting documentation provided by DHS; DHS performed a risk assessment and found that there was no risk to USCG systems pose any significant cybersecurity risk to DHS or USCG because they operate on the DoD network/ platform (DoDIN), not on the DHS network/platform (OneNet). The OIG has not integrated the supporting documents that DHS provided to them into their assessment of DHS’s information security program. As a result, the OIG’s independent assessment does not accurately reflect the maturity of DHS’s cybersecurity program and its assessment of risks.DHS made strides in all four Federal Information Security Management Act (FISMA) metrics: Identify, Protect, Detect, and Respond & Recover. We are focusing on regaining “Managing Risk” rating for Identify. We will achieve this by finalizing the implementation of Continuous Diagnostics and Mitigation (CDM) capabilities and by the sustained focus of the new Chief Information Officer (CIO) on resolving expired Authorizations to Operate (ATO) and closing high risk Plans of Action & Milestones. DHS currently receives hardware and software asset management data directly from 9 out of 11 Components. Authorization Management is being improved by working intensively to support Component success. DHS actively monitors the ATO status of FISMA systems and usage of improper operating systems in monthly cybersecurity reports and works with every Component to manage risks and vulnerabilities. The CIO is personally supporting a few Components in this effort. The Department has updated and communicated its Information Security Performance Plan for FY2021, allowing agency executives more visibility on IT risks impacting their mission space.

Independent Assessment

In a May 28, 2020 memorandum, the Deputy Under Secretary for Management formally documented its acceptance of the risk to allow the Coast Guard to meet the FISMA requirements in accordance with the Department of Defense’s reporting requirements. The Deputy Under Secretary for Management’s May 28, 2020 decision directly and adversely affects our ability to evaluate the Department’s information program in an enterprise-wide approach under this year’s OIG reporting metrics, which are based on the NIST’s CSF. Further, we maintain that the FISMA statute does not include language to permit shifting agency responsibilities to another agency. This rating does not include the Coast Guard when evaluating the overall effectiveness of DHS’ information security program for FISMA. For FY 2020, DHS’ information security program was effective because the Department earned a maturity rating of “Managed and Measurable (Level 4)” in three of five functions. DHS can improve the effectiveness of its information security program because the components are still not executing all of the Department’s policies, procedures, and practices. For example, we identified:

1. systems are being operated without authority to operate;
2. known information security weaknesses are not being mitigated timely;
3. security configuration settings are not being implemented for all systems; and
4. components also used unsupported operating systems and did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems.

Since 2019, our independent contractor has performed fieldwork at six selected components and rated three components’ information security programs as “ineffective” because the components achieved below “Level 4 - Managed and Measurable" in three of five functions, under the current OIG reporting metrics.

FY2020 Annual Cybersecurity Performance Summary

Department of Housing and Urban Development

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	1	0	0
E-mail	7	15	3
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	49	14	20
Loss or Theft of Equipment	4	0	0
Web	9	1	0
Other	25	11	15
Multiple Attack Vectors	1	1	0
Total	**96**	**42**	**38**

CIO Self-Assessment

This summary highlights what the Department of Housing and Urban Development (HUD) has done to adjust to COVID-19 and how the Agency has implemented safe cybersecurity practices.

While adjusting to COVID-19 shutdown and telework, HUD took significant measures to inform HUD employees of the dangers of cyber vulnerabilities and risks of remote work by increasing monitoring for cybersecurity awareness and conducting multiple employee trainings and malware and phishing campaigns. Additionally, HUD's OCIO developed Agile solutions to the operational challenges of remote work, while also releasing memos to remind HUD employees of best practices against cyber threats, telework related cyber risks, and providing up to date information on software and security management.

In May of 2020, David Chow, Chief Information Officer, issued a Risk Based Decision (RBD) Local Area Network (LAN P-209) and Wide Area Network (P223) Risk Acceptance for Extension of HUD Account Management for Network Lockouts Due to the COVID-19 pandemic. This memorandum requested an extension of the Risk Based Decision (RBD) from April 16, 2020 on the HUD information system policy authorizing the extension of current HUD information system policy from May 2, 2020 to July 31, 2020, which disables inactive user accounts in the Local Area Network (LAN P-209) and the Wide Area Network (WAN P-223) due to the continued mandatory telework for HUD employees. The memorandum is being refreshed to extend the scheduled expiration of user ID passwords in FY 2021.

Independent Assessment

The Department of Housing and Urban Development's (HUD) increased in overall maturity from defined to consistently implemented in FY 2020, which is HUD's first time achieving this overall maturity level. HUD OIG observed progress in key CIO initiatives in FY 2020 to address HUD's information security (IS) and IT challenges, which resulted in HUD's increased maturity. Throughout FY 2020, HUD created remediation plans and took corrective actions for many prior year HUD OIG recommendations. The HUD OCIO had early successes in modernizing parts of the HUD infrastructure, such as the data centers, cloud adoption, and a mainframe system. The progress in cloud adoption, such as FHA Catalyst, demonstrated positive movement that should help HUD modernization efforts. However, HUD's IS program was evaluated as not effective because it did not reach a managed and measurable maturity level. Challenges, such as senior leadership having limited time in their roles, and incomplete or inaccurate system documentation, contributed to the lack of an effective IS program. The large number of HUD legacy systems continued to create challenges to the IS program, as they are resource-intensive and introduce the most risk to the computing environment. HUD's enterprise and IT risk management program, which did show some improvement in FY 2020, lacked the maturity to fully prioritize resource allocation. In addition, HUD struggles with procurement challenges, affecting the ability to timely award IT contracts and provide proper oversight when modernization efforts are pursued. HUD OIG recommends that HUD continue to prioritize the IS program focusing on assessing and maturing the FISMA domains. Leadership continuity, along with proper oversight and accountability are essential for HUD to continue on the path to achieve an effective IS program.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	6	1	2
E-mail	610	378	246
External/Removable Media	0	1	0
Impersonation	1	0	0
Improper Usage	175	199	114
Loss or Theft of Equipment	42	14	3
Web	82	9	2
Other	270	184	81
Multiple Attack Vectors	2	1	2
Total	**1,188**	**787**	**450**

CIO Self-Assessment

In response to the COVID-19 pandemic in March 2020, the Department of Justice (DOJ) initiated its Continuity of Operations, Contingency, and Incident Response Plan. The maximum telework mandate put to test the Department's secure remote access infrastructure and IT modernization investments. DOJ sustained its security posture by implementing additional network security controls; allowing limited, monitored use of split tunnel access; increasing user awareness training; and assessing vendors' risk management practices. DOJ's Justice Security Operations Center (JSOC) adopted a hybrid telework model to sustain full monitoring service capabilities while maintaining a safe work environment for security analysts. The JSOC detects and blocks millions of malicious emails per month, and continuously tests and measures the effectiveness of DOJ's security awareness programs through its enhanced enterprise phishing simulation platform implemented in FY 2020.

Independent Assessment

During FY 2020, the Department of Justice's (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: 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, 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.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	2	1	1
E-mail	35	25	17
External/Removable Media	0	1	0
Impersonation	0	0	0
Improper Usage	81	96	111
Loss or Theft of Equipment	100	97	80
Web	16	2	5
Other	50	100	109
Multiple Attack Vectors	0	0	2
Total	**284**	**322**	**325**

CIO Self-Assessment

In FY 2020, to enhance the maturity of its cybersecurity program, and at the same time mitigate new cybersecurity risks associated with expansion of telework under the COVID-19 national emergency, the Department of Labor (DOL) continued advancements in the following areas: Inventory of Systems and Assets, Security Incident Response, ISCM, Security Management, and Enterprise IT initiatives.

DOL implemented enterprise solutions to enhance IT asset management, automation, and to facilitate near real-time awareness of vulnerabilities. This included ServiceNow enhancements, as well as implementation of additional DHS CDM tools for vulnerability management

DOL transitioned its Security Operations Center to provide 24x7 monitoring and incident response capabilities, adapted and matured client endpoint security to account for the increased teleworking environment, implemented DLP mechanisms to alert on potential data exfiltration activities through file transfers and through email, and increased Web Application Firewalling of DOL cloud hosted publicly available application servers.

DOL also implemented cloud-based solutions to enable secure information sharing and manage access in a remote environment. This included enhancements to SharePoint, OneDrive, and deployment of MS Teams.

In response to maximum telework for DOL staff, DOL increased the use of RSA tokens to maintain continuity and security when onboarding new staff, and to support existing personnel with expired PIV cards who were unable to obtain new credentials in person. DOL provided additional security awareness trainings and quarterly phishing exercises to address increased cybersecurity risks faced by remote users. These measures allowed DOL to seamlessly shift 95 percent of staff to telework, with uninterrupted delivery, while keeping cybersecurity a top priority.

Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, the implementation of DOL's information security program and practices (policies, procedures and tools) was determined as "not effective." During the period of our testing, we identified 36 deficiencies within four of the five cybersecurity functions and six of the eight FISMA metric domains based on a selection of 16 federal and 4 contractor information systems, and entity wide testing. Based on the maturity level for each security function that CyberScope calculates, it was determined that DOL's information security program was not effective because three cybersecurity functions were rated as Consistently Implemented (Level 3) Not Effective, and the remaining two cybersecurity functions were assessed as Managed and Measurable (Level 4) Effective.

FY2020 Annual Cybersecurity Performance Summary

Department of State

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	36	10	6
E-mail	3,082	1,043	289
External/Removable Media	2	1	1
Impersonation	0	0	3
Improper Usage	514	609	631
Loss or Theft of Equipment	22	8	3
Web	353	158	110
Other	541	495	192
Multiple Attack Vectors	10	52	16
Total	**4,560**	**2,376**	**1,251**

CIO Self-Assessment

Department of State (DOS) remains a target of interest for a variety of global threat actors. DOS established an enterprise Cyber Security Work Group (CSWG) to advance strategic cyber governance and improve operational cyber posture across DOS. DOS commissioned a Risk & Resiliency Work Group (RRWG) to continually identify and manage the intrinsic risk associated with execution of its global mission. The CSWG and RRWG report to a CIO led IT Executive Council and through it to the DOS Enterprise Governance Board thereby linking leadership actions at the strategic and tactical levels of the organization. DOS continued aggressive implementation of its risk management initiatives. The Cyber Risk Management Program was codified into a permanent office expanding its ability to provide cyber risk guidance to DOS IT leadership. DOS remains committed to adopting the effective cybersecurity practices and embedding them into the agency's culture.

DOS response to COVID-19 was swift and successful. Operating on a global basis presented logistical challenges associated with implementing mission enabling changes for a dispersed workforce unable to physically report to their office. DOS was able to expand on existing remote access solutions successfully all the while tracking and evaluating the risk of each technical change. As COVID-19 driven dynamics are changing, the applicable technical changes are under continuous risk review and assessment to determine if the risk level accepted at the outset remains current or if additional changes are needed. CISA has cited the FY 2020 updates to DOS cyber risk management strategy as an exemplar for the federal community. DOS plans to continue refining and implementing the risk management indicators and reporting necessary to guide leadership decisions. DOS continues to enhance its cybersecurity posture and collaborative partnerships across the federal government.

Independent Assessment

The information security program of the U.S. Department of State was evaluated as not effective. The assessment scope included a selection of the Department's major information systems. OIG's independent contractor found that the Department generally implemented pieces of an information security program that supports the operations and assets of the Department. However, the assessment identified numerous areas where controls and processes could be improved. The assessment resulted in 29 recommendations with identified weaknesses across most domains and functional areas. Despite this, the Department demonstrated measurable improvement in the Risk Management, Configuration Management, Incident Response, and Contingency Planning domains.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	9
Loss or Theft of Equipment	3	0	3
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	**4**	**0**	**12**

CIO Self-Assessment

The Department of State OIG network supports 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. OIG operates an independent network that is aligned with the Risk Management Framework and FISMA requirements.

OIG faces cybersecurity risks that are common across the Federal Government. 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 FY20 to mitigate cybersecurity risks and bolster defenses.

To ensure the secure continuity of its mission during the COVID-19 national emergency, OIG authorized and implemented additional collaboration technologies to foster improved productivity and communication among staff and security personnel. OIG upgraded its VPN devices and clients to improve security, stability, and performance of remote connections. OIG also increased its cybersecurity related outreach and continued phishing exercises to ensure all staff remain vigilant of current threats. Click-rates further reduced, improving user resilience against threats.

OIG implemented a cloud-based user and entity behavior analytics solution to identify, detect, and investigate advanced threats, compromised identities, and insider actions. OIG also enhanced its disaster recovery strategies and resiliency of OIG systems and resources by implementing additional backup and failover capabilities.

OIG completed a comprehensive review and update of its Cybersecurity Framework implementation, completing an analysis of desired states for the various maturity metrics. OIG received a rating of “Managing Risk” on the FY20 Q4 Risk Management Assessment.

Independent Assessment

As independent auditors, we conducted 2020 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. OIG has witnessed significant but balanced growth in resources (people, processes and technology) to support OIG mission. 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 all domain areas. OIG followed through with 2019 IG FISMA Metrics recommendations to implement advanced technologies (aligned with IT Supply Chain strategy) 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-premise and cloud environments. FY2020 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.

FY2020 Annual Cybersecurity Performance Summary

Department of the Interior

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
Protect	At 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	FY18	FY19	FY20
Attrition	0	2	1
E-mail	4	8	10
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	143	255	164
Loss or Theft of Equipment	18	13	0
Web	68	17	19
Other	172	263	169
Multiple Attack Vectors	2	2	0
Total	**407**	**560**	**363**

CIO Self-Assessment

DOI prevailed during an unprecedented year. The Department closed 96% outstanding audit items to include four (4) major items (2016-ITA-062, 12.a.OCIO & 2.b.OCIO, GAO-19-384 #19 & 20) in the DOI Enterprise Cybersecurity Risk Management Program. In addition, DOI closed all actions for DHS CISA Binding Operational Directives (BOD-17-01, BOD-18-01, BOD-18-02, BOD-19-02) and two Emergency Directives (ED 20-02, ED-20-03, ED-20-04) on time and with no identified deficiencies. In FY20, DHS CISA identified DOI as one of the top five agencies in federal government in completing DHS BODs and EDs.

Since the commencement of remote telework due to COVID in March 2020, the Department established new virtual personnel on-boarding practices, processes, and procedures. New solutions permitted hundreds of personnel to be rapidly hired and deployed, most notably including 80 Wildland firefighters and emergency first responders.

DOI successfully migrated to a new email and collaboration solution just in time to successfully support COVID-19 contingency operations. OCIO migrated 85,000 user mailboxes containing 458 TeraBytes (TB) of email, 71 TB of shared drive data, 2,241 shared sites, and 28,500 mobile devices. OCIO increased the capacity of the Virtual Private Network (VPN) for all DOI remote users as well as maintaining secure access to agency systems.

DOI continues efforts to improve security and address Risk Management Assessment (RMA) measures for High Risk areas. DOI continues to improve incident response, is implementing the CDM dashboard, and is establishing an IT supply chain risk management program. It is expected these actions will markedly improve DOIs cybersecurity posture.

Independent Assessment

We conducted a Performance Audit over DOI’s information security program to determine the effectiveness of such program for the FY ending September 30, 2020. The scope of the audit included the following Bureaus and Offices: Bureau of Indian Affairs (BIA), Bureau of Land Management (BLM), 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 Special Trustee for American Indians (OST), and U.S. Geological Survey (USGS). DOI had 158 operational unclassified information systems, and we randomly selected 11 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, Identify, Protect, Detect, Respond, and Recover. However, the program was not effective as weaknesses were identified three of five function areas, Identify, Detect, and Recover. The Protect and Respond function areas were effective.

Weaknesses were noted in the FISMA domain areas of risk management, configuration management, data protection and privacy, information system continuous monitoring, and contingency planning domains.

FY2020 Annual Cybersecurity Performance Summary

Department of the Treasury

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	1	0	4
E-mail	5	54	7
External/Removable Media	0	1	1
Impersonation	1	6	0
Improper Usage	114	14	139
Loss or Theft of Equipment	16	10	5
Web	5	3	1
Other	43	54	49
Multiple Attack Vectors	0	0	0
Total	**185**	**142**	**206**

CIO Self-Assessment

The mission of the Department of the Treasury (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 IT assets and networks. The likelihood of risk realization is magnified by the expansion of telework under the COVID-19 national emergency and the continuing evolution in the volume, sophistication, and frequency of cyber threats.

Treasury leadership remains engaged in the development of plans to address these risks. In FY20, the Department 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 developed the Enterprise Cyber Risk Management program to manage vulnerabilities that can be exploited to affect Treasury assets, especially critical under increased telework. Treasury created enhanced risk profiles for all 19 HVAs in FY20 to provide leadership with greater visibility into associated risks, and with DHS completed one RVA, seven SARs and one HVA assessment of nine HVAs. In addition, Treasury completed option year one for CDM DEFEND, and is currently calculating the AWARE score and integrating Identify and Access Management (IAM) information to the Federal Dashboard.

Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidance, and NIST standards and guidelines, Treasury established and maintained its information security program and practices for its unclassified systems and collateral NSS for the five Cybersecurity Functions and eight FISMA Metric Domains. However, the program was not effective according to DHS criteria and as reflected by the eight exceptions noted within three of the five Cybersecurity Functions and within six of the eight FISMA Metric Domains. We assessed IAM, Security Training, ISCM, and Incident Response as Managed and Measurable (Level 4); and we assessed Risk Management , Configuration Management, Data Protection and Privacy, and Contingency Planning as Consistently Implemented (Level 3). Overall, we assessed the Treasury's Information Security program and practices for unclassified systems and collateral NSSs as Consistently Implemented (Level 3).

FY2020 Annual Cybersecurity Performance Summary

Department of Transportation

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	1	2	3
E-mail	27	15	6
External/Removable Media	0	1	3
Impersonation	2	0	1
Improper Usage	172	92	85
Loss or Theft of Equipment	93	0	1
Web	174	40	25
Other	324	157	130
Multiple Attack Vectors	10	4	5
Total	**803**	**311**	**259**

CIO Self-Assessment

During FY2020, the Department of Transportation (DOT) identified multiple areas of risk impacting agency systems and took action to respond to and mitigate those risks. To improve e-mail security, DOT reprioritized resources to acquire services to increase agency implementation of trusted e-mail capabilities from 46% to greater than 98%, including retiring unneeded legacy e-mail services. DOT also identified systems with end-of-life software, acquired extended support to facilitate patching of critical and high vulnerabilities, and accelerated efforts to upgrade or retire the end-of-life systems. To effect improvements in system authorization and risk management, the DOT CIO established an enterprise cybersecurity contract and began efforts to increase use of the vehicle by DOT component organizations. To address weaknesses in cloud security, DOT collaborated with the FedRAMP PMO Director to provide specialized training on the FedRAMP program and processes to DOT cybersecurity personnel, enhanced visibility into acquisition of cloud services by leveraging FITARA IT spend processes, and invested in a cloud access security broker (CASB) service to begin securing DOT employee access to and use of authorized cloud services. To address long-standing issues surrounding contingency planning and recovery, DOT realigned resources and has begun efforts to focus on improvements to that aspect of the DOT cybersecurity program. Regarding DOT's response to COVID-19, the agency successfully transitioned personnel to maximum telework without significant increase in risk. However, DOT did identify opportunities to improve security controls and protections for personnel working remotely and acquired an advanced endpoint protection security solution for deployment of the capability to customers of the DOT CIO's IT Shared Services organization.

Independent Assessment

Based upon our audit of DOT's information security program, including its performance in the function areas, we concluded that overall, 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. DOT has, for the most part, formalized and documented its policies, procedures, and strategies; however, DOT continues to face significant challenges in the consistent implementation of its information security program across the organization. In addition, controls need to be applied in a comprehensive manner to information systems across DOT in order to be considered consistent and fully effective by achieving at least a rating of Level 4, Managed and Measurable.

Accordingly, we continue to see security deficiencies similar in type and risk level to prior years and an overall inconsistent implementation of the security program. Consequently, we noted weaknesses in each of the eight Inspector General FISMA Metric Domains encompassing the Department's Agency-wide program. The audit identified continuing deficiencies related to risk management, configuration management, identity and access management, data protection and privacy, security training, information security continuous monitoring, incident response and contingency planning practices designed to protect mission critical systems from unauthorized access, alteration, or destruction.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	3	0	0
E-mail	358	162	233
External/Removable Media	4	14	0
Impersonation	3	2	0
Improper Usage	75	13	21
Loss or Theft of Equipment	362	498	302
Web	239	89	7
Other	732	49	375
Multiple Attack Vectors	0	0	3
Total	**1,776**	**827**	**941**

CIO Self-Assessment

As COVID-19) reshaped how the Department of Veterans Affairs (VA) works operates, VA staff adapted to ensure continuity of care and operations for our Veterans. This involved working with staff and accommodating their unique situations during COVID-19, 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)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. But during COVID-19, it was 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, we 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 (RMF) 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.

FY2020 Annual Cybersecurity Performance Summary

Election Assistance Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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 Election Assistance Commission (EAC) completed migration from an on-premise network infrastructure that was hosted primary by GSA to a new cloud infrastructure, which has significantly increased visibility and adaptability for EAC, as well as allowed a seamless cutover to 100% remote work in March 2020. Additionally, EAC has established a dedicated cybersecurity program to address cybersecurity responsibilities within the agency.

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. Although, EAC Office of Information Technology generally has policies for its information security program, its implementation of those policies was not fully effective to ensure the confidentiality, integrity, and availability of the Agency's information and information systems.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	5	2	11
External/Removable Media	0	0	0
Impersonation	1	0	0
Improper Usage	41	102	15
Loss or Theft of Equipment	63	33	37
Web	14	0	8
Other	41	63	36
Multiple Attack Vectors	0	1	3
Total	**165**	**201**	**110**

CIO Self-Assessment

The Environmental Protection Agency (EPA) achieved the Risk Management Assessment Overall “Managing Risk” level in FY2020 and system level risks, including those to HVAs supporting mission essential functions, have been determined to be at acceptable levels. Known risk areas EPA continues to aggressively address include insufficient resources; insider threats; remote users; ex-filtration defenses; legacy and emerging technologies; acquisitions processes, and sub-optimal staffing levels, skills, and organization.

EPA is working with the CDM program to improve EPA’s capabilities by providing continuous monitoring (CM) tools and dashboards. EPA invested significant resources to transition CM tools to O&M and improve data quality. EPA explored and leveraged cloud and host capabilities to improve visibility of device and user behavior. EPA, working with DHS, initiated host vulnerability scanning capabilities, implemented alternative authentication mechanisms to provide multi-factor capabilities for replacing passwords, and expanded use of virtual desktops for users and administrators to address gaps caused by expanded teleworking under the COVID-19 national emergency. EPA also implemented processes to ensure new users working remotely were properly vetted prior to obtaining access to systems.

Independent Assessment

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

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

- Risk Management - The EPA has not completed its corrective actions to:
  - Implement an enterprise Software Asset and Configuration Management capability to align license-entitlement data with software inventories.
  - Establish a control to validate that PO&AMs are created for weaknesses identified from vulnerability testing.
- Configuration Management - The EPA has not updated information security procedure documentation to reflect the security-control requirements of NIST SP 800-53, Revision 4, issued on January 22, 2015.
- Identity and Access Management - The EPA has not officially established its Project Management Office, which will define ownership, plan resources, and monitor progress of the Agency’s identity, credential, and access management program. In addition, we found that the EPA lacks implemented processes for monitoring privileged user activity and for authorizing external access to the sampled system evaluated for this domain.

FY2020 Annual Cybersecurity Performance Summary

Equal Employment Opportunity Commission

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Consistently Implemented
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	FY18	FY19	FY20
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	1	0	0
Web	0	0	0
Other	1	1	1
Multiple Attack Vectors	0	0	0
Total	**3**	**1**	**1**

CIO Self-Assessment

In FY 2020, the Equal Employment Opportunity Commission (EEOC) continued modernizing its technology infrastructure and mitigating major risks. The pandemic presented significant operational challenges to extend remote work capabilities in a safe, robust, and secure manner. To meet these new challenges, the Agency reconfigured existing assets, retired legacy systems, sped up the delivery of collaboration initiatives, and introduced new technologies where needed. These efforts included expanding our cloud presence, deploying virtual desktop technology, enhancing mobile device management, and extending our VPN for full Agency use. The EEOC also increased enterprise cybersecurity visibility and resilience, and significantly improved logging, event monitoring, and incident handling in its cloud tenant. The Agency continued implementing newly technologies, including advanced threat protection, improved malware and vulnerability scanning, enhanced access control lists, and network access control services. The EEOC improved its security posture through compliance with government cybersecurity requirements, including BoDs 20-01 and 18-01, critical threats in EDs 20-02, 20-03, and 20-04, along with FISMA and DHS' Cyber-Hygiene programs. As staff have not been in the office for seven months, full deployment of PIV multi-factor authentication is now projected for completion before the end of FY 2021.

Independent Assessment

We determined EEOC's information security program is effective and provides reasonable assurance of adequate security. The results of our performance audit concluded that EEOC's information security program is generally compliant with the FISMA legislation and is consistent with the functional areas outlined in the NIST Cybersecurity Framework.

FY2020 Annual Cybersecurity 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		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
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 Export-Import Bank (EXIM) deployed state of market enterprise security capabilities in the areas of Data Loss Prevention, Security Event Incident Management, and Phishing simulation. These enhancements to the EXIM environment allow for comprehensive and secure management in order to promote continuous authorizations, risk-based decision making, and real-time awareness of the state of security across the bank. In alignment with the PMA for modernizing the Government mission-support services and cloud smart strategies, EXIM continues to enhance its architecture to provide secure access to applications hosted in the cloud while increasing the use of shared service offerings from external agencies. To support the unique mission of EXIM, the bank's long-standing telework capabilities provide a comprehensive and secure set of services for EXIM staff to support the mission remotely. Overall, the bank's experience during the COVID-19 national emergency and the agency's response to unprecedented new challenges has been largely positive and effective. EXIM established a COVID-19 task force that meets weekly to conduct knowledge sharing, address agency concerns, and develop strategy and action plans. EXIM strengthened its incident response policies and procedures conducting comprehensive training exercises to mitigate the increased risk of incidents that come with universal telework, including lost or compromised equipment, loss of availability to the network, etc. EXIM enhanced its cybersecurity awareness and phishing training programs by highlighting telework-specific risks in its awareness program and implementing state of the market automation and dynamic training at the point of failure to increase user vigilance regarding cyber threats. EXIM continues to enhance its Information Security Continuous Monitoring program through our partnerships with the DHS Shared Services and CDM programs and the Small and Micro Agency Council.

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 Risk Management, ISCM, and Contingency Planning metric domains, we determined its information security program was effective as we evaluated the majority of the FY 2020 IG FISMA Reporting Metrics at the Managed and Measurable (Level 4) or higher maturity levels.

FY2020 Annual Cybersecurity Performance Summary

Farm Credit Administration

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	4
Loss or Theft of Equipment	5	15	3
Web	0	0	0
Other	2	0	0
Multiple Attack Vectors	0	0	0
Total	**8**	**15**	**7**

CIO Self-Assessment

The Farm Credit Administration (FCA) continues to mature its cybersecurity Risk Management Program. Risks are identified from several sources, such as on-demand risk assessments, open-source intelligence, assessment and authorization, penetration tests, and after-action incident reviews. The risks of highest significance to the organization center on FCA's safety-and-soundness, mission-essential function and the ability for its examiners to access and transfer relevant examination-related information to the FCA network for further evaluation. FCA is also tracking risks aligned with the NIST Cybersecurity Framework. The FCA risk register is reviewed weekly by the CIO, the senior Office of Information Technology (OIT) staff, the Chief Data Officer, and the Program Manager of the FCA Office of Examination Operations Risk Program. During these reviews, changes in risk factors are discussed. The CIO discusses high-priority concerns with senior FCA staff members and FCA Board Members, as appropriate. Over this past FY, has been able to close eight risks due to the implementation of mitigations and refinement of how risks are captured. During this time, FCA has identified 13 additional risks, some as a result of the COVID-19 pandemic's effect on the agency's IT risk posture. FCA has also continued to leverage the previous FY's hiring of a dedicated privacy professional to ensure maximum implementation of privacy controls. To ensure the security of examination data, FCA conducts intrusion prevention, encrypts sensitive database columns, and ensures TLS-encrypted connections with 100% of our institutions. FCA also conducts mobile device management, including policy enforcement and remote wipe of lost devices.

Independent Assessment

The OIG contracted with an independent audit firm to conduct an audit on the 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,
- Implementation of risk-based security controls,
- Corrective action for significant information security weaknesses,
- Change Control Board,
- 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 in all five functions for FCA to continue to improve the program and made appropriate recommendations.

FY2020 Annual Cybersecurity Performance Summary

Federal Communications Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	8	0	1
E-mail	5	4	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	2	1	14
Loss or Theft of Equipment	11	8	5
Web	5	20	5
Other	16	12	61
Multiple Attack Vectors	0	0	0
Total	**47**	**45**	**87**

CIO Self-Assessment

The Federal Communications Commission (FCC) recognizes the following cybersecurity risks to the agency:

- Security ATOs not completed for all organization operated systems.
- Findings and Recommendations from IG's FY 2019 FISMA Evaluation.
- "Critical" and "High" vulnerabilities not remediated within their stated timelines.
- Lack of two-factor PIV credential for user authentication.
- Disaster recovery/continuity planning due to COVID-19 mandatory telework.
- 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:

- Developed a 3-year plan to get to 100% ATOs by the end of 2022.
- Implemented corrective action plans for all findings from IG's FY 2019 FISMA Evaluation.
- Created a plan to remediated "Critical" and "High" vulnerabilities by September 2021.
- Currently identifying the best solutions for multi-factor authentication.
- Expanded agency capacity and resources on network infrastructure to allow for increased usage of Virtual Desktop Infrastructure.

Independent Assessment

The FY 2020 FISMA evaluation included the FCC's network (i.e., FCCNet), the FCC's core financial management system (i.e., Genesis), and the FCC's incident ticketing and change management system (i.e., ServiceNow). While the FCC made improvements to processes within its overall Information Security Program since the FY 2019 FISMA evaluation in the areas of identity and access management (i.e., separation of duties analysis, reviewing access for privileged users, and user authorization), data protection and privacy (i.e., testing the FCC's Data Breach Response Plan), and incident response (i.e., documentation of incidents), an independent auditing firm and the FCC Office of Inspector General (OIG) determined that the FCC's overall program was ineffective in FY 2020. Specifically, the independent auditors assessed the FCC's security processes related to the five National Institute of Standards and Technology (NIST) Cybersecurity Functions and determined that one function (Recover) was at a maturity Level 4, Managed and Measurable; three functions (Identify, Protect, and Respond) were at a maturity Level 3, Consistently Implemented; and one function (Detect) was at a maturity Level 2, Defined. Additionally, the independent auditors identified reportable control weaknesses in four of the eight domain areas within the five functions. The independent auditors did not identify any significant reportable weaknesses in the Data Protection and Privacy, Security Training, Incident Response, and Contingency Planning domains. Going forward, the independent auditors 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.

FY2020 Annual Cybersecurity Performance Summary

Federal Deposit Insurance Corporation

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	0	3
External/Removable Media	0	1	1
Impersonation	1	0	0
Improper Usage	101	77	56
Loss or Theft of Equipment	0	0	0
Web	4	0	3
Other	8	2	0
Multiple Attack Vectors	0	0	0
Total	**115**	**80**	**63**

CIO Self-Assessment

The Federal Deposit Insurance Corporation (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 2020 include further development of key policies and procedures impacting essential security control areas (e.g., release of a new Identity, Credential, and Access Management Program Strategy and supporting architecture); integrating the Risk Management Framework (RMF) into business processes, contracts and projects; and embedding the RMF into Chief Information Officer Organization (CIOO) lifecycle planning and governance as those functions take shape. There is also a multi-year CIOO initiative to improve the FDIC's information security and data management practices to protect the security of FDIC information and facilitate appropriate information sharing. Through a collaborative effort between the CIOO and FDIC operating divisions, the Data Protection Program will offer further protections to FDIC sensitive information and data by categorizing and labeling FDIC information and data.

Independent Assessment

The FDIC's information security program was operating at a Maturity Level 3 (Consistently Implemented). 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.

The FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines. The FDIC also took or was working to take steps to strengthen its security program controls following the FISMA audit conducted in 2019. For example, the FDIC completed actions to address 10 of 12 unimplemented recommendations made in prior-year FISMA audit reports; developed new or revised security policies and procedures in key areas; and completed work on a new backup data center. However, the audit identified security control weaknesses that limited the effectiveness of the FDIC's information security program and practices and placed the confidentiality, integrity, and availability of systems and data at risk. The highest risk weaknesses involved the need for FDIC to: fully define its ERM governance, roles, and responsibilities; integrate privacy into its RMF; ensure POA&Ms are addressed timely; consistently reassess risk acceptance decisions; ensure software is authorized before it is installed on the network; ensure sensitive data, including PII, is adequately protected; ensure all outsourced systems are properly categorized, authorized to operate, and monitored; and complete annual security assessments of cloud-based systems. The audit resulted in eight recommendations intended to improve the effectiveness of FDIC's security program and practices. The FDIC concurred with all eight recommendations and planned to complete corrective actions by December 2021. The FDIC was also working to address an additional two recommendations from prior FISMA audit reports.

FY2020 Annual Cybersecurity Performance Summary

Federal Energy Regulatory Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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	1	0	1
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**1**

CIO Self-Assessment

In FY 2020, Federal Energy Regulatory Commission (FERC) continued to make significant investment in maintaining, evolving and maturing our risk-based, cost effective cybersecurity program. Some highlights include: 1) Completed deployment of a DLP solution to monitor and prevent sensitive data exfiltration; 2) Completed biennial Controlled Unclassified Information (CUI) training for all staff, ensuring understanding of methods and process to protect sensitive data; 3) Implemented secure baselines for 12 new and existing technologies; 4) Implemented a secure coding analysis review process for all custom development. 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 the annual evaluation of FERC's unclassified information security program to assess the effectiveness of unclassified information security policies, procedures, and practices within five information security functions (Identify, Protect, Detect, Respond, and Recover). The OIG determined that the Commission had an effective information security control environment. Specifically, FERC had “Optimized” information security controls functions (Level 5) in Identify, Detect, and Respond, and “Managed and Measurable” information security control functions (Level 4) in Protect and Recover.

FY2020 Annual Cybersecurity Performance Summary

Federal Housing Finance Agency

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	FY18	FY19	FY20
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	26	13	5
Web	0	0	0
Other	0	1	2
Multiple Attack Vectors	0	0	2
Total	**26**	**15**	**9**

CIO Self-Assessment

The Federal Housing Finance Agency (FHFA) continued to make progress toward meeting Cybersecurity CAP goal metrics in FY 2020 while operating primarily as a remote workforce since March 2020 due to the COVID-19 national emergency. In FY 2020 FHFA achieved a preliminary RMA rating of "Managing Risk," and the OIG independent review concluded that "FHFA generally 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."

In FY 2020 FHFA increased the frequency and scope of phishing tests and associated user training and has continued to reduce the use of passwords for internal systems, which is progress towards employing user-based enforcement for network access.

The expansion of telework due to the COVID-19 national emergency required limited changes to FHFA's security practices in order to maintain operations in a remote environment. Most notably was 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 has a multi-factor authentication solution in place as a backup that minimizes this risk and additionally FHFA implemented host-based inspection of all laptops connecting remotely via VPN.

Independent Assessment

An Independent Public Accounting (IPA) firm under contract and supervision of the Federal Housing Finance Agency (FHFA) OIG completed a performance audit to evaluate the effectiveness of FHFA's Information Security Program and practices and respond to the DHS FY 2020 IG FISMA Reporting Metrics, dated April 17, 2020. The IPA's methodology included testing the effectiveness of selected security controls implemented in a subset of systems in accordance with the NIST SP 800-53, 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 five of the eight domains in the FY 2020 IG FISMA Reporting Metrics. As a result, the IPA made seven recommendations to assist FHFA in strengthening its information security program.

FY2020 Annual Cybersecurity Performance Summary

Federal Labor Relations Authority

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

Incidents by Attack Vector	FY18	FY19	FY20
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 Federal Labor Relations Authority (FLRA) successfully navigated FY 2020 with no reported Cybersecurity incidents. We were able to meet the requirements outlined by ED 20-04. The Agency had no findings in 2019 and is actively working to address findings from 2020. Our users continue to reach out with Cybersecurity questions, forward us suspicious email, and to report possible Cybersecurity incidents. As an agency we continue to provide our users with ongoing education and to encourage them to take an active part to ensure the agency maintains a positive information security stature. COVID-19 did not introduce any new security risks as the FLRA already maintained a robust telework infrastructure.

Independent Assessment

The Federal Labor Relations Authority, Office of Inspector General completed its annual FISMA assessment for FY 2020. The FISMA engagement assessed all NIST 800-53 (Rev. 4) controls that were referenced in the Office of Management and Budget's CyberScope requirements. Our testing included inquiry, observation, and assessing configuration settings over selected controls. The assessment resulted in four new findings for this current fiscal year. Those deficiencies were in the areas of: policies and procedures needing to either be developed or updated, timely remediation of vulnerabilities, documentation of position risk designations, as well as ensuring that users' rights are reviewed timely to ensure that users' access rights are commensurate with their job descriptions. Our test procedures were not significantly or directly impacted by the COVID pandemic and was able to be completed timely, while meeting our reporting deadlines.

FY2020 Annual Cybersecurity Performance Summary

Federal Maritime 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	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
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	4
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**4**

CIO Self-Assessment

The Federal Maritime Commission (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 IT assets, the agency has deployed security standards in response to DHS' BOD and continues to reduce internal and external vulnerabilities through the implementation of the CDM program cybersecurity tools and services and through implementing MTIPS.

Independent Assessment

The overall IG assessment rating is "effective" for the FMC. In the IG's FY 2020 FISMA audit, the OIG identified one audit finding and two corresponding recommendations. Specifically, although the FMC has various information technology security policies and procedures, several had not been updated/reviewed in a timely manner, or they were lacking from not being developed into a formalized policy. The IG recommended the FMC develop, review and update, as necessary, the applicable policies and procedures in accordance with NIST and agency requirements.

FY2020 Annual Cybersecurity Performance Summary

Federal Mediation and Conciliation Service

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

Incidents by Attack Vector	FY18	FY19	FY20
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	4
Multiple Attack Vectors	0	0	0
Total	**0**	**2**	**4**

CIO Self-Assessment

We have followed our cyber-security framework action plan and have secured the services of 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. We have implemented a Managed Security Services Provider (MSSP) for continuous monitoring in FY 2020. This has allowed us to respond in a comprehensive manner to any incidents identified by the MSSP. We have identified and submitted our HVAs per BOD 18-02 and integrated them into our cyber security framework. By performing these actions, we believe we have made significant progress towards achieving level 4 maturity for these metrics.

Independent Assessment

We have followed our cyber-security framework action plan and have secured the services of several contractors to perform comprehensive cyber-security assessments to include suggested paths to successfully remediate any actions identified. We have also procured software that will perform automated inventory of software, hardware, and provide alerts of any software changes or remediation needs to system administrators. We plan to replace any deficient processes with automated services where possible in FY 2021 and beyond. By performing these actions, we believe we will make significant progress towards achieving level 4 maturity for these metrics.

FY2020 Annual Cybersecurity Performance Summary

Federal Mine Safety and Health Review Commission

Framework	CIO Rating	IG Rating
Identify	At Risk	Managed and Measurable
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	FY18	FY19	FY20
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 Federal Mine Safety and Health Review Commission (FMSHRC) remains vigilant of the potential vulnerabilities identified by security vulnerabilities reported to the agency. FMSHRC remains committed to migrating our network to a cloud platform in addition to using cloud solutions to mitigate risk. Due to the current COVID-19 pandemic, FMSHRC has had to pause such implementations. In accordance with the plan as outlined by the Executive Director, we will move forward with such implementations as soon as it is safe to do so. FMSHRC's entire workforce is currently working remotely due to the pandemic. However, FMSHRC does have required implementations in place to prevent infiltrations and penetrations into our network with settings at our Domain-based Message Authentication Reporting and Conformance (DMARC) with p=reject, other security software, and the requirement of credentialing when accessing and Webservers, to include Microsoft. We will monitor daily activities on our network and continue to apply applicable patches as they are released while working with our Internet Service Provider (ISP) to mitigate vulnerabilities. FMSHRC remains committed to adhering to all security guidelines and will continue to update our aging infrastructure with the previous plans outlined prior to COVID-19. Staff assigned to the Executive Director’s direct supervision has internal monitoring protocols in place as well.

Independent Assessment

The FMSHRC deployed and have in-progress information security compliance projects to address information security concerns. Symantec End-Point Protection is deployed to endpoint for antivirus, data exfiltration, application control/file, and registry access, email malware, and phishing abatement. Network Access Control (NAC) is implemented as a solution to Port Block/Collect and Parse MAC Address preventing DHCP Inclusion to network access. Network Access Protection (NAP) is implemented as a solution to detect and alert on the connection of an unauthorized hardware asset. Microsoft Defender Advanced Threat Protection is implemented as a risk-based approach to the discovery, prioritization, and remediation of endpoint vulnerabilities and misconfigurations. Continuous Diagnostics and Mitigation deployment is implemented to identify, track, and abate critical cyber risks.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	12	4	11
Loss or Theft of Equipment	18	13	3
Web	0	0	0
Other	2	5	6
Multiple Attack Vectors	0	0	0
Total	**32**	**22**	**20**

CIO Self-Assessment

In FY 2020, the Federal Retirement Thrift Investment Board (FRTIB, or "the Agency") made significant advances in 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 FISMA domains. Based on the maturity ratings across the eight (8) domains, the independent auditor concluded that FRTIB had an effective information security program in FY 2020. The Agency has taken the security program and FISMA maturity extremely seriously and moved forward with multiple efforts to improve its information security posture and maturity during FY 2020.This was done through the further definition and implementation of new or better processes across all security domains, as well as the definition of metrics to assess the effectiveness of the program.

Of the ten CAP goals for FY 2020, the Agency has achieved all but one;--Software Asset Management. 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 2021 (and beyond), with a goal of improving and maintaining the Agency's maturity across all FISMA domains.

In regards to COVID-19 response, the Agency was well positioned to transition its employees and contractors to full telework when the COVID-19 national emergency was declared. Over the last several years, the Agency made significant investments in the network infrastructure, VPN capabilities, security monitoring, and collaboration tools. As such, the transition to remote work was primarily focused on transitioning contractors in Agency contact centers to remote work in order to continue to provide services to TSP participants and beneficiaries. The Agency implemented changes to IT hardware and software applications to support, secure, and monitor the contact center contractors working remotely and reduce any associated risks as much as possible.

Independent Assessment

The independent assessment of the Federal Retirement Thrift Investment Board (FRTIB)'s information security program concluded that seven (7) of the eight (8) FISMA domains are rated at a Level 4 (Managed and Measured) and the overall program is effective. This conclusion was determined through an independent assessment of entity-wide and system specific controls, with a particular focus on three (3) of FRTIB's information systems.

FRTIB achieved an effective information security program through its continued efforts to define and implement processes across all eight (8) FISMA domains. Furthermore, FRTIB developed performance metrics and supporting processes to monitor and measure the effectiveness of its information security program.

The independent auditor issued two (2) recommendations to assist FRTIB in making improvements to areas where the associated reporting metrics did not achieve a Level 4 rating or control deficiencies were identified.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	1	0	1
E-mail	3	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	18	7	17
Loss or Theft of Equipment	0	2	1
Web	0	0	0
Other	1	0	0
Multiple Attack Vectors	0	0	0
Total	**23**	**10**	**19**

CIO Self-Assessment

The Federal Trade Commission (FTC) continues to manage Mission Essential Functions (MEF) risk by leveraging FedRAMP CSP, such as cloud identity management and IT service management. The Agency continues to make progress converting legacy IT to modern cloud service offerings, but still relies on legacy IT hosted in its on-premise data centers. Examples of progress include decommissioning the FTC legacy E-Filing service with a modern web service, moving Agency e-mail from the local Data Center to a CSP, implementing additional monitoring to improve detection capabilities, and upgrading legacy IT to current industry standards. In addition, the agency updated policies for incident identification to mitigate risk of significant deviations from expected use of FTC systems. 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. The Agency will continue to pursue IT capabilities with strong authentication, inspection, and encryption at-rest and in-motion to minimize adverse impacts from network latency or limited bandwidth.

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 eight 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 that FTC's information security program and practices were effective for the period October 1, 2019, to September 30, 2020.

FY2020 Annual Cybersecurity Performance Summary

General Services Administration

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Managed and Measurable
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	FY18	FY19	FY20
Attrition	1	1	1
E-mail	5	4	3
External/Removable Media	0	0	0
Impersonation	0	0	1
Improper Usage	49	65	68
Loss or Theft of Equipment	0	0	0
Web	3	2	7
Other	21	24	22
Multiple Attack Vectors	0	0	0
Total	**79**	**96**	**102**

CIO Self-Assessment

The cybersecurity threat landscape and the risks they pose to information, information systems, and services is dynamic and ever increasing. The further democratization of data and systems out of traditional boundaries to the edge and the expansion of telework under the COVID-19 national emergency further exacerbates this challenge, but also presents opportunities to modernize IT and improve cybersecurity.

Risks and related mitigations faced in FY2020 are below:

1-Phishing: Continuous Phishing Campaign; Binding Operational Directive (BOD) 18-01 Email and web-security security; Email URL analysis and Executable sandboxing

2-Hardware and Software Supply Chain: Agency-wide governance of Supply Chain Risk Management (SCRM) including an 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; Pilot program with DOD to perform third party SCRM risk assessments of suppliers.

3-OT/IOT Security: Network segmentation to break out user and OT/IOT networks; further enhancing via implementation of micro segmentation technology; Hardware/Software device testing via Device Testing Lab

4-Malware and Cyber Hacking: Security enhancements to identify and block incidents early in the cyber-kill-chain. Key technologies include 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 (IR);Enterprise Logging with machine learning; Cyber threat hunting

5-Remote Work Security: VPN Load Balancing; External DNS Resolver solution; Two Factor Authentication; Mobile and Workstation EDR solutions;Covid-19 Situational Threat Monitoring via custom dashboards tracking Distributed Denial of Service (DDOS), VPN usage, and security threats; Remote on-boarding of new hires; New MTIPS Gateway

Independent Assessment

Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, GSA has consistently implemented its information security program and practices (policies, procedures, and tools) for the five cybersecurity functions and eight FISMA domains. We identified seven deficiencies within one of the five cybersecurity functions and two of the eight FISMA metric domains based on a selection of five federal and five contractor information systems and entity-wide testing. GSA closed six of eight prior-year recommendations. Based on the maturity level that CyberScope calculates, it was determined that GSA's information security program was effective because one cybersecurity function was assessed at Optimized (Level 5), three cybersecurity functions were assessed at Managed, and Measurable (Level 4), and the remaining one was assessed at the Consistently Implemented (Level 3), which is how OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency defined an effective program.

FY2020 Annual Cybersecurity 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	

CIO Self-Assessment

As a micro agency, the Gulf Coast Ecosystem Restoration Council (GCERC) has partnered with Federal Shared Services to provide risk mitigation. The largest risk to GCERC is endpoint protection. GCERC is implementing CISA's CDM along with contracted services to provide endpoint protection and monitoring. GCERC maintains a continuous monitoring program to ensure the information assurance program is effective.

Incidents by Attack Vector	FY18	FY19	FY20
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**

Independent Assessment

The Department of the Treasury (Treasury) OIG contracted with an independently certified public accounting firm 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, 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 eight FISMA metric domains. RMA found that the Council's information security program and practices were effective for the period July 1, 2019 through June 30, 2020. 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, as well as the CIO's direct involvement in every IT security decision and security controls, and the simple IT structure of stand-alone computers and service vendors. IA's effectiveness tests found no exceptions.

FY2020 Annual Cybersecurity Performance Summary

Institute of Museum and Library Services

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
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	FY18	FY19	FY20
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

Major focus areas for the Institute of Museum and Library Services (IMLS) in Fiscal Year (FY) 2020 were to build upon the security controls implemented in FY 2019, update system security plans to reflect its recent migration of mission critical data and applications to the cloud, and to ensure continuous monitoring of security controls and their effectiveness.
IMLS is expected to complete the updates to System Security Plans for all its systems and initiate a comprehensive security assessment and authorization by an independent third party by the end of FY 2021.
Independent network monitoring services have detected a couple of cyber security risks with IMLS' guest Wi-Fi network in Q4 of FY 2020. This network was only used by agency guests and employees' personal devices. This guest Wi-Fi network is physically separate from IMLS.gov network and has no impact on imls.gov endpoints. IMLS scanned the network with end point protection and it was determined that none of the devices or components on the network were compromised. As a long-term mitigation strategy, IMLS OCIO has decommissioned the current IMLS Wi-Fi network and appliance, and will implement a firewall solution as a Wi-Fi controller with additional security controls in place. The new Wi-Fi system with more robust access points is expected to be operational by end of Q2 FY 2021.
IMLS' digital transformation and modernization work throughout the past few fiscal years has facilitated a seamless transition of all business functions and staff to be 100% telework ready during the COVID-19 pandemic. Access to agency resources is available only through dual factor authentication and mission critical data is encrypted both in motion and at rest.

Independent Assessment

The scope of this audit covers the IMLS GSS. The independent auditor 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 supporting documentation as it pertains to the IMLS GSS. 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 on which IMLS develops sound policies and procedures so the agency can institutionalize them at the highest level possible.

FY2020 Annual Cybersecurity Performance Summary

Inter-American Foundation

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	1	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**	**1**	**0**

CIO Self-Assessment

The biggest risk was scanning vulnerabilities and applying required patches. The Inter-American Foundation (IAF) procured a remote scanning tool to install the agent on user laptops, providing the vulnerabilities to the cloud account even when the user was connected to the IAF network. This managed the risk and IAF was able to apply patches in several different ways.
Secondly, user training on PII and security and protection of data was provided to users while working from home.
IAF increased its bandwidth from 10MB to 30MB and is now in the process of increasing to 100MB.

Independent Assessment

IAF's information security program was evaluated as part of the Fiscal Year (FY) 2020 FISMA Audit. This audit included an evaluation of five out of seven FISMA reportable systems at IAF. The audit determined that 87 of the 100 instances of the selected NIST SP 800-53 Rev. 4 security controls were properly implemented. Therefore, the independent auditors deemed IAF's information security program effective.

FY2020 Annual Cybersecurity Performance Summary

International Boundary and Water Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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	0	0	1
Multiple Attack Vectors	0	0	0
Total	**1**	**0**	**1**

CIO Self-Assessment

The International Boundary and Water Commission, United States and Mexico, U.S. Section (USIBWC) consists of one Moderate Security Level General Support System (GSS) and two High Security Level Supervisory Control and Data Acquisitions (SCADA) operational systems. All information security programs comply with the laws and regulation established by FISMA, as amended, and standards prescribed by OMB and NIST. The USIBWC is in the process of achieving a renewed ATO designation for our GSS and SCADA systems which operate our International Wastewater Treatment Plants located in Nogales, AZ and San Ysidro, CA. The agency anticipates renewed GSS and SCADA System ATO designations as soon as possible in FY 2021. The USIBWC is in the process of developing and implementing an ongoing Information Security CDM service for all three systems which will augment existing CDM services provided to the agency through DHS. The USIBWC has awarded a contract for CDM services to be implemented by the end of FY 2021. The USIBWC enabled multifactor authentication of system applications to comply with best practices and add an extra layer of security during the expansion of telework under the COVID-19 national emergency. The USIBWC has also performed recent phishing exercises relating to COVID-19 to continue training our users on how to detect and report phishing attempts against the USIBWC network.

Independent Assessment

The information security program of the International Boundary and Water Commission was evaluated as not effective. The assessment scope included all of USIBWC's major information systems. OIG's independent contractor found that USIBWC generally implemented pieces of an information security program that supports the operations and assets of USIBWC. However, the assessment identified numerous areas where policies were not current and where controls and processes could be improved. The assessment resulted in twenty-five recommendations with identified weaknesses across all domains and functional areas.

FY2020 Annual Cybersecurity Performance Summary

International Trade 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	Consistently Implemented
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	1	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	1	2
Loss or Theft of Equipment	1	0	0
Web	0	0	0
Other	2	4	1
Multiple Attack Vectors	0	0	0
Total	**4**	**6**	**3**

CIO Self-Assessment

Over the past few years, the Commission has worked to embrace telework and a mobile workforce. Numerous technologies like a PIV-authenticated VPN, remote datacenter, software, and Software-as-a Service cloud solutions have been implemented to support the remote workforce. These technologies, along with an IT service desk and business unit procedures and policies designed with a remote service model in mind, placed the Commission in a strong position to handle the telework expansion 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, temporary staff, etc). In the past, these non-PIV users were unable to connect to the Commission’s VPN.

Independent Assessment

During the COVID-19 pandemic, the Commission has continued to effectively manage software across all compatible devices, while identifying and remediating vulnerabilities, with staff being 100% remote. The Commission continues its efforts in managing all hardware on the network as well as strengthening its incident response and management processes to minimize risks to the confidentiality, integrity, and availability of the network. The Commission has a strong security and awareness program, which trains all users on current cyber security threats involving social media, identity management, cloud application systems, and best practices for protecting a home network.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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 US Friendship Commission (JUSFC) is a nano agency with four FTEs and limited budgetary authority. The COVID-19 pandemic required all FTEs to go on fulltime, indefinite telework. JUSFC is a grantmaking agency that does not perform classified work. The existing IT infrastructure has allowed for secure remote work, enabling the agency to protect its electronic assets and unclassified daily mission work.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Japan-United States Friendship Commission was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
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

Narrative Assessment of the Marine Mammal Commission Information Security Program

The Marine Mammal Commission is a micro agency consisting of three Commissioners with a nine-member advisory committee, the Committee of Scientific Advisors on Marine Mammals. The Commissioners and Committee members serve part-time as special government employees. The Commission is 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 and, as such, it believes that its exposure to cybersecurity risks is small. 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, should the need arise.

2) The Commission's official personnel records are maintained by the General Services Administration, Commissions and Boards. Supervisor records are maintained in locked files by 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 use of 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 are equipped with routinely updated antivirus software.

Independent Assessment

Narrative Assessment of the Marine Mammal Commission Information Security Program

The Marine Mammal Commission is a micro agency consisting of three Commissioners, with a nine-member advisory committee, the Committee of Scientific Advisors on Marine Mammals. The Commissioners and Committee members serve part-time as special government employees. The Commission is 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 and therefore has limited risks of information security breaches or a need for extensive assessments. 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, should the need arise.

2) The Commission's official personnel records are maintained by the General Services Administration, Commissions and Boards. On-site records are maintained in locked files accessible only to the Chief Administrative Officer and the Executive Director.

3) In FY 2012 the Commission initiated use of 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 run routinely updated antivirus software.

The Commission will continue to consult with its IT contractor and others, as appropriate, to identify cost-effective ways in which information security can be further improved.

FY2020 Annual Cybersecurity Performance Summary

Merit Systems Protection Board

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	8	3	1
Loss or Theft of Equipment	2	1	2
Web	0	1	0
Other	0	1	1
Multiple Attack Vectors	0	0	0
Total	**10**	**7**	**4**

CIO Self-Assessment

In FY20, the Merit Systems Protection Board (MSPB) took several steps to strengthen its cybersecurity program. We maintained the MOA with DHS including weekly scans of our internet-accessible addresses and systems, as well as weekly Cyber Hygiene, HTTPS, and Trustworthy Email reports. MSPB continued to attend weekly CISA CyberLiaison and SOC calls. We maintain all available IPSS services (TA, MEF, DSS) on our MTIPS circuit and are actively engaged with our ISP for regular maintenance and incident resolution. MSPB filled our vacant CIO position in July 2020. We also updated our computer login banner, and actively reviewed existing policies and procedures and developed new ones to comply with COVID-19 guidance. New procedures were created for IRM staff to access our HQ data center and the network equipment that we actively manage on premise. In addition, we implemented cloud-based DDoS mitigation for our public web servers. Regarding expanded telework, we implemented a new FedRAMP-certified web conferencing solution and issued specific rules of behavior for employees and external participants. We are also working to deploy new Windows 10 laptops to replace legacy Windows 7 devices. Annual computer security training was at 100% participation and delivered to all employees through a vendor that allowed IRM to remotely deliver and monitor employee access. Independent auditors assessed MSPB's GSS which was conducted remotely through file-sharing and VTC. As a result, a conditional ATO for our GSS was granted pending the assessment results. In FY21-22, MSPB plans to implement the next generation business applications; this will sunset all remaining client-server servers and systems. Finally, MSPB continues to coordinate with DHS on expanding our CDM program and using the new dashboard functions with Windows 10 machines.

Independent Assessment

An independent auditor examined the MSPB GSS. They assessed 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 supporting documentation as it pertains to the MSPB GSS. 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 on which MSPB develops sound policies and procedures and the advanced maturity levels, so the agency can institutionalize them at the highest level possible.

Upon completion of the audit, it is apparent that MSPB has put forth a concerted effort in securing the organization's GSS environment. MSPB has improved on or maintained a positive rating in the following areas:

- MSPB has established and implemented risk management strategies and processes.
- ISCM processes are established by assigning activities to MSPB stakeholders with defined frequencies and security requirements.
- MSPB has made a noticeable improvement over FY19 in both Incident Response and Data Protection and Privacy domains.
- MSPB ensures that basic security training is monitored and provided to MSPB stakeholders at least annually.

However, certain discrepancies and process improvements are required to be corrected and implemented by the MSPB Information Security Team.

FY2020 Annual Cybersecurity Performance Summary

Millennium Challenge Corporation

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	2	2
Loss or Theft of Equipment	0	1	0
Web	1	0	0
Other	0	2	1
Multiple Attack Vectors	0	1	0
Total	**2**	**6**	**3**

CIO Self-Assessment

1. Access control: Due to COVID-19 restrictions, Millennium Challenge Corporation (MCC) waived expiring PIV certificates. Users are unable to physically renew their PIV certificates during mandatory telework operations.
2. Network monitoring: Increased network health monitoring and reporting initiated to ensure reliability of the network.
3. MCC has managed the network efficiently to ensure operational capability.

Independent Assessment

MCC’s information security program was evaluated as part of the FY 2020 FISMA Audit. This audit included an evaluation of four out of seven FISMA reportable systems at MCC. The audit determined that 115 of the 120 instances of the selected NIST SP 800-53 Rev. 4 security controls were properly implemented. Therefore, the independent auditors deemed MCC’s information security program as effective.

FY2020 Annual Cybersecurity Performance Summary

Morris K. Udall Foundation

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	FY18	FY19	FY20
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

We have contracted with an independent firm to conduct a FISMA assessment, which is now in the final stages of being completed. The resulting security assessment report will be used to identify high, moderate, low and risk-based controls that we will address. A plan will be developed to meet all deficiencies. Our agency was in a good position when the mandatory telework order was given in April 2020. VPN bandwidth and collaboration platforms were our two biggest issues. We did have Microsoft Teams as part of our software inventory; however, it had not been deployed at the time we went into mandatory telework status. Rollout and training of Microsoft Teams was completed in April 2020. Our existing VPN solution at the time our telework status changed lacked the bandwidth to support all our staff simultaneously. We moved our VPN gateway to our offsite data center location and configured a dedicated firewall for VPN needs.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Morris K. Udall Foundation was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment. The Morris K. Udall Foundation will explore contracting with an independent assessor in FY 2021.

FY2020 Annual Cybersecurity Performance Summary

National Aeronautics and Space Administration

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	FY18	FY19	FY20
Attrition	2	1	5
E-mail	5	7	11
External/Removable Media	0	0	2
Impersonation	0	0	0
Improper Usage	180	1,329	1,165
Loss or Theft of Equipment	23	15	3
Web	30	3	17
Other	76	108	417
Multiple Attack Vectors	1	6	6
Total	**317**	**1,469**	**1,626**

CIO Self-Assessment

The National Aeronautics and Space Administration (NASA) is responsible for ensuring information technology’s secure use in support of its mission objectives. As the Agency transitioned to telework during the COVID-19 national emergency, NASA’s efforts focused on providing modern and secure IT services to the Agency’s remote workforce. This included adapting cybersecurity processes and requirements in order to ensure capabilities and functions were available remotely, such as system patching and onboarding activities for new hires. Additionally, NASA expanded capabilities via enabling secure, standardized work processes and deploying mobile and audio services for collaboration. The Agency also delivered a near-seamless (99 percent availability) remote connection experience to approximately 40,000 users per day (a 233 percent increase from 12,000 users daily during normal, pre-pandemic operations) in support of mandatory telework.

Independent Assessment

During our Fiscal Year (FY) 2020 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 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. Because of our evaluation, we have determined that information security continues to remain a significant challenge for NASA. While NASA continues to make progress in securing its networks and information systems, its cybersecurity program remains ineffective when judged using OMB's model, which requires agencies to achieve a level 4 maturity (managed and measurable) to be considered effective. In the five functional areas reviewed during this evaluation, NASA information systems remain vulnerable to internal and external cybersecurity threats.

FY2020 Annual Cybersecurity Performance Summary

National Archives and Records Administration

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

Incidents by Attack Vector	FY18	FY19	FY20
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	2	3	0
Other	4	7	2
Multiple Attack Vectors	0	0	0
Total	**8**	**10**	**2**

CIO Self-Assessment

IT security has improved but remains a challenge for the National Archives and Records Administration (NARA). NARA's information security policies, procedures, and practices provide adequate protections that are generally effective. However, in some cases we lack the formal documentation necessary to ensure that our policies and strategies are consistently implemented. Because of long-standing risks in NARA IT security, we declared IT security a material weakness in internal controls in fiscal years 2015 through 2020. NARA continues to improve its ability to protect the confidentiality, integrity, and availability of NARA resources. In FY 2020, NARA made significant progress toward the authorization of seven additional moderate impact systems. These systems have been assessed and will be authorized in Q1 FY 2021, and the agency expects to achieve authorization for 100% of its FISMA reportable systems in FY 2022. Additionally, NARA awarded a contract to implement the Department of Homeland Security's CyberArk tool to enforce two-factor authentication using the Federal PIV card for users with elevated security responsibilities. NARA has strategically reduced the number of external email services used by the agency to broadcast communications to both internal and external audiences. By doing so, NARA aligned external email services, with the enhanced email security requirements of BOD 18-01 and has achieved 100% compliance in FY 2020. COVID-19 has presented many challenges to support 100% remote telework. To meet the demands of the workforce and minimize adverse impact on the business, NARA had to modify some processes. However, strong compensating controls were implemented to secure the enterprise.

Independent Assessment

Overall, NARA has not changed from last year, having five domains assessed at the lowest "ad-hoc" level, and three domains assessed one level above the lowest at the "Defined" level. However, NARA continues to stress its commitment to improving information security throughout the agency and is making steady progress to that end. NARA also continues to work to address open OIG audit recommendations related to information security.

In FY 2020, NARA continued its progress toward a more mature information security program, including the following:

- Acquiring additional Information System Security Officer (ISSO) resources, which helped the agency create and maintain up-to-date security documentation for many systems in the sample.
- Improving its master system inventory process to include more accurate and comprehensive system information compared to prior years.
- Introducing new channels of communication to update information security stakeholders on the newest security topics and changes in IT policies and procedures.

However, to fully progress towards being 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. Consistent implementation of security controls throughout the agency can only be achieved when there are sound and reliable policies and procedures, the foundational levels of a mature information security program. Please see the OIG Narrative for further details.

FY2020 Annual Cybersecurity Performance Summary

National Capital Planning Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	2	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	2	0
Multiple Attack Vectors	0	0	0
Total	**1**	**4**	**0**

CIO Self-Assessment

At the beginning of FY 2020, the National Capital Planning Commission (NCPC)'s annual cyber strategy was to continue to modernize its business practices to include implementing cloud-based solutions and becoming more aggressive in its cyber practices. While work towards these two goals ensued during Q1 and Q2, efforts quickly shifted on 3/18/2020, when, due to the pandemic, for the safety of the staff, the NCPC implemented a 100% telework status for the agency. The transition to 100% telework resulted in a need for a real-time collaboration platform, which introduced several cyber challenges such as bandwidth utilization and remote access to the cloud environment. To address these challenges and support the additional network load inherent in cloud solutions, the NCPC increased its bandwidth on the MTIPS circuit from 30mbps to 100mbps. While we are aware that it is preferred to connect to the agency's chosen FedRAMP-approved collaboration platform via VPN on the MTIPS circuit for monitoring and inspection purposes, accessing the cloud from the VPN caused service degradation that impacted the staff's ability to expediently access agency resources and effectively collaborate with one another. Therefore, the NCPC made a risk-based decision to allow staff to access the cloud platform on an agency-issued and managed device from a public network over TLS. The agency's solution aligns with Option 1 as described in the TIC 3.0 Interim Telework Guidance.
To maintain the agency's secure virtual operations in a telework environment, the IT team implemented a modified patch management schedule. NCPC Divisions were assigned designated days each week to log onto the VPN to be scanned and obtain weekly patches. The team also disabled PIV enforcement for authentication to user machines and the NCPC network. The team determined it would be unable to provide remote administration support if machine-based enforcement was enabled for PIV logon; therefore, PIV enforcement was disabled.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the National Capital Planning Commission was not performed for FY 2020, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

National Council on Disability

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

Incidents by Attack Vector	FY18	FY19	FY20
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 National Council on Disability (NCD) is aware of the very real security issues to be considered around teleworking. These issues are wide-ranging: the accidental introduction of viruses to the office environment, increased exposure to Internet attacks, even acting as a backdoor into the heart of the NCD network. Teleworkers and NDC in general take these issues, and protection against them, very seriously. The remote PCs have been protected against the internet and the NCD network is protected from the remote PC by the following mechanisms:

- Security Policy
- Protecting Remote PCs
- User Education
- Firewalls
- Virus Protection

Independent Assessment

NCD understands that the most important asset of an organization is information, and ensuring the confidentiality and integrity of associated operational processes. NDC also understands that cyberattacks have emerged as a major risk to individuals, businesses, and governments alike. It is especially important for our information security program that all the staff in the agency are aware of these information security issues with proper training and initiatives.

NCD’s information security program is working to implement crucial functions for our agency’s Risk Management, Continuous Monitoring, Policies and Training, and related areas that will enable the smooth application’s operation applied to NCD’s IT systems. These functions ensure the safety of NCD’s data and protect our technology assets to ensure they are functioning correctly.

To better protect our information, NCD has installed or applied the correct software to secure and safeguard protected applications. NCD has also started to make changes to allot more funding to our information security program.

FY2020 Annual Cybersecurity Performance Summary

National Credit Union Administration

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	1	0
E-mail	3	3	5
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	7	3	0
Loss or Theft of Equipment	21	4	6
Web	7	0	0
Other	4	5	1
Multiple Attack Vectors	0	0	0
Total	**42**	**16**	**12**

CIO Self-Assessment

While the National Credit Union Administration (NCUA) made progress in 2020, the following key risk areas are the most significant:

1. Data Management Security: NCUA published an Enterprise Data Program policy to manage enterprise data as a strategic asset throughout its full lifecycle to include security, privacy, and records management.
2. Legacy Application Security: NCUA continued the development and testing of more secure modern applications that will replace four legacy applications in FY 2021.
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.
4. HVAs: Three of NCUA's HVAs are legacy applications that will be decommissioned and replaced with more secure modern applications in 2021.

NCUA's workforce is predominately full time remote which equipped the agency to transition to an entirely remote workforce during the pandemic.

NCUA took the following steps to reduce risks during the transition to full remote work:

- Reviewed and adjusted, as needed, all employee telework agreements.
- Issued guidance on the use of agency-approved collaboration tools while sharing and discussing agency information.
- Published knowledge articles for NCUA employees and contractors on the secure use of NCUA approved collaboration tools.
- Issued a reminder to NCUA employees and contractors to raise awareness around increased COVID-19-related phishing campaigns.

Independent Assessment

NCUA OIG assessed the NCUA in all function areas and underlying domains identified in the FY 2020 IG FISMA Reporting metrics as they pertain to four of six of the NCUA's FISMA reportable systems and its overall information security program. The NCUA has continued to strengthen its information security program during FY 2020. Specifically, we determined the NCUA is effective in its security awareness and training program, its contingency planning and its incident response program. In addition, NCUA addressed and closed 12 of the 21 recommendations from the FY 2019 FISMA report. NCUA is in the process of addressing and resolving the nine remaining recommendations from the FISMA 2019 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 identified areas for improvement this year in the areas of risk management, access management, and configuration management, considering the compensating controls in place, we deemed NCUA's overall information security program effective. In addition, the weaknesses we identified during this year's evaluation, in combination, do not have a significant enough impact on NCUA's overall information security program for us to consider it ineffective.

The recommendations we are making in the OIG's FY 2020 FISMA report should help the NCUA continue to improve the effectiveness of its information security program.

FY2020 Annual Cybersecurity Performance Summary

National Endowment for the Arts

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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	1
External/Removable Media	0	0	0
Impersonation	1	0	0
Improper Usage	0	1	3
Loss or Theft of Equipment	0	1	0
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	**1**	**3**	**4**

CIO Self-Assessment

Primary cybersecurity risks to the National Endowment for the Arts (NEA) during FY 2020 include phishing emails and ransomware. Prior to FY 2020, the NEA had already deployed solutions to mitigate these risks, including web and email content filtering and 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 FY 2020, the NEA has taken several steps to significantly improve cybersecurity capabilities to protect the confidentiality, integrity and availability of agency systems by beginning to adopt Zero Trust methodology. The NEA continued to move critical assets to FedRAMP approved CSPs. The agency implemented new vulnerability scanning software that is capable of scanning agency devices anywhere as long as they have an internet connection. The agency implemented a SIEM and CASB tool that is fully integrated into all of the agency systems producing logging data. An identity access management system is currently implemented and waiting for a return to work to onboard all agency personnel. The NEA also hired a full-time federal Chief Information Security Officer to continue to guide the NEA security program. Security program reviews have demonstrated progress this year in the agency's security posture and integration of tools that greatly improve cybersecurity incident monitoring, prevention, and response.

The COVID-19 national emergency caused the NEA to expand its telework capacity to 100%. During this time, the agency began deployment of the new private access platform (which is set to be completed in Q1 of FY 2021) to replace the agency's current VPN solution. The agency developed a TIC 3.0 use case in FY20 and implemented some of the features of the TIC 3.0 user case to provide a greater layer of protection on agency devices in the field during COVID-19.

Independent Assessment

The independent auditor 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 2020. Based on test procedures performed, the independent auditor identified weaknesses in all IG FISMA metric domains, resulting in ten recommendations. Therefore, the independent auditor determined that the NEA needs to take action in order to improve its information security program to become effective (Level 4: Managed and Measurable).

FY2020 Annual Cybersecurity Performance Summary

National Endowment for the Humanities

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

Incidents by Attack Vector	FY18	FY19	FY20
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	0	0	5
Multiple Attack Vectors	0	0	0
Total	**3**	**1**	**5**

CIO Self-Assessment

In FY 2020, the National Endowment for the Humanities (NEH) faced the COVID-19 pandemic challenges and diverted our IT department's resources to transitioning and supporting 100% of the staff to full remote capabilities. This included developing and scaling secure file sharing into the cloud for the enterprise, expanding BYOD procedures to ensure remote capabilities across the enterprise, revising onboarding policies and procedures, updating our acceptable use policy, and integrating the updated policies as part of NEH's Annual Security Awareness and Privacy training program. Even with resource challenges, NEH has not only maintained its security posture from last year but has also made a few improvements to the overall risk summary areas from FY 2019.

The RMA Overall Summary page in FY 2019 identified a High Risk under the Protect category, Credentialing and Authorization domain. NEH's additional RBAC implementation and revised policies have allowed changes to the centralized access management value for both Unprivileged and Privileged users, from 0% in FY 2019 to 100% in FY 2020. This effectively changed the ratings from High Risk to Managing Risk and has raised the overall Credentialing and Authorization rating. NEH no longer has any Security Domains listed as High Risk for FY 2020.

NEH also made improvements in other areas. For example:
FY19 risk: The CAP Goal for "A7. Automated Access Management" has a rating of 0 due to not having a centralized access management solution.

FY20 status: NEH's Access Management now has many automated security features in the centralized access management solution.

NEH's CISO rolled out new Security Awareness and Privacy Training 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.

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, budgetary constraints in previous fiscal years and competing priorities for NEH IT staff have contributed to the agency's inability to fully implement core elements of risk management (Identify), ISCM (Protect), and contingency planning (Recover), which impedes the overall effectiveness of the NEH information security program. Current NEH leadership has committed personnel and budgetary resources to support the initiation 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 in progress. However, much of the manpower and resources slated for the A&A were reallocated to support priorities necessitated by the COVID-19 pandemic. Consequently, the A&A schedule has been extended.

FY2020 Annual Cybersecurity Performance Summary

National Labor Relations Board

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

Incidents by Attack Vector	FY18	FY19	FY20
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	2	1	1
Multiple Attack Vectors	0	0	0
Total	**2**	**2**	**1**

CIO Self-Assessment

The Agency utilized an independent assessor (Shared Service) to test and validate the Agency's HVA controls in accordance with NIST 800-53A revision 4. In addition, all our FISMA reportable systems are regularly tested and have a valid ATO. During the past year the Agency continued its transition into the Microsoft cloud environment and now the majority of our IT assets are located within Azure. We continued to develop and document processes and implement automated capabilities to protect the confidentiality, integrity and availability of agency resources. In FY 2019, we acquired a new IT support contract that provided security resources and helped the agency improve our rating during the annual FY 2020 FISMA Inspector General audit.

The Agency continued to protect our IT resources and has been especially diligent through this period of increased telework. The CIO provided regular communication to all users reminding them about agency policy and provided guidance and best practices for safely accessing and handling agency data. The Agency is 100% compliant with BOD 18-01 and has taken immediate action with all CISA Emergency Directives related to patching of vulnerabilities. We also continued to work with the CDM program to safeguard, secure, and strengthen our security posture. In addition, we enforce VPN usage with approved GFE and required multi-factor authentication in compliance with HSPD-12 for network logon. To actively monitor agency resources in real time, we utilize several cloud-based solutions.

Independent Assessment

For the past several years, the OCIO made steady progress in improving the NLRB's IT security processes and maturity. For this year's review, the OCIO met at least the "managed and measurable" level across the five IT security functions and obtained an overall maturity level assessment of "effective." This steady improvement over an extended period of time represents a significant effort on the part of the OCIO security staff.

FY2020 Annual Cybersecurity Performance Summary

National Mediation Board

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

Incidents by Attack Vector	FY18	FY19	FY20
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	0	1	0
Multiple Attack Vectors	0	0	0
Total	**0**	**1**	**1**

CIO Self-Assessment

The National Mediation Board continues to undertake initiatives towards meeting the CIO FISMA metric objectives. The agency's new contractor team of technical and security professionals are performing updates to the agency's security policies and procedures, as well as identifying gaps and solutions. This has resulted in several initiatives for the year that are aimed to improve our overall security posture and compliance with OMB, DHS, and FISMA requirements. Since the last reporting, the agency has deployed an enterprise solution for all laptops, aimed specifically at protecting its remote staff against known malicious websites and IP addresses as they work in the field. The agency also implemented role-specific training for Tier 2 staff. With the addition of contractor information security personnel, the agency is able to better manage its security posture. Going forward, the agency will implement MTIPS in FY 2021, which will improve the agency's internet security for both onsite and remote users.

Independent Assessment

An independent evaluation of the status of the information technology (IT) cybersecurity program for the National Mediation Board was not performed for FY 2020, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

National Science Foundation

Framework	CIO Rating	IG Rating
Identify	Managing Risk	Optimized
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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	2	2	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	0	0
Loss or Theft of Equipment	0	0	0
Web	3	0	1
Other	1	1	3
Multiple Attack Vectors	0	0	0
Total	**7**	**3**	**5**

CIO Self-Assessment

National Science Foundation (NSF) seamlessly transitioned to secure remote work during the COVID-19 pandemic, with minimal staff required to be in the headquarters building. NSF continued security awareness campaigns to keep staff informed about emerging phishing and scamming efforts related to COVID-19. NSF maintained its daily security operations while reviewing and analyzing threats through the COVID-19 perspective to protect NSF systems. NSF leveraged DHS intelligence on specific COVID-19 threats to increase its vigilance and security posture during the pandemic. NSF improved existing processes and support capabilities for remote staff including software management, troubleshooting and vulnerability management. While presented with challenges in FY20, NSF proactively and continuously assessed security controls and targeted strategic areas for strengthening the security and privacy programs.

Independent Assessment

To assess whether the NSF effectively implemented its agency-wide Information Security Program and practices, an independent auditor conducted a performance assessment. The auditor 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 2020 Inspector General FISMA Reporting Metrics.

Based on the audit, NSF's Information Security Program was effective for FY2020. The driving factor for the assessment is the improved maturity of the USAP information security environment, which directly impacted NSF's overall ratings. Improvements were achieved by developing and implementing corrective action plans in response to prior year deficiencies. To become more effective, NSF will implement a Plan of Action and Milestones (POA&M) to address findings identified during the FISMA audit.

FY2020 Annual Cybersecurity Performance Summary

National Transportation Safety Board

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

Incidents by Attack Vector	FY18	FY19	FY20
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	0	2	0
Multiple Attack Vectors	0	0	0
Total	**1**	**5**	**1**

CIO Self-Assessment

The National Transportation Safety Board (NTSB) has taken several steps to reduce or mitigate risk during this telework expansion under the COVID-19 national emergency. The agency launched the COVID-19 Risk Assessment Dashboard, which provides COIVD-19 data to all NTSB staff members. The data provided on this website is broken down into three categories: Risk Assessment, Risk Assessment Map and National Database.
The mission of our agency is to investigate transportation accidents in the following areas: Aviation, Marine, Highway, RPH (Railroad, Pipeline and Hazardous Materials. This dashboard displays calculations and color ratings based on the NTSB COVID-19 Risk Management protocol for investigative activity using CDC, state and local data. This information assists the agency with planning safe and efficient transportation investigations.

Independent Assessment

Upon completion of the audit, it is apparent that NTSB has gone through extensive efforts to secure the organization’s 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;
- The technical implementation of the Information Security Continuous Monitoring program is well established and executed in near real-time;
- Vulnerability scanning of agency information systems and assets has been established and is performed according to FISMA security requirements and frequencies;
- NTSB has established an effective configuration management program for its information systems by employing the use of automated mechanisms that provide on demand and real-time baseline, security configuration requirements, and risks views of the entire agency infrastructure;
- Automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, ISCM, and Configuration Management programs;
- NTSB ensures that security training is monitored and provided to NTSB stakeholders at least annually and given to NTSB personnel according job functions and levels of access; and
- NTSB has established and maintained an effective Incident Response program that includes validated processes for responding, containing, and reporting security incidents to oversight agencies such as US-CERT and DHS.

Notwithstanding, certain discrepancies and process improvements are required to be corrected and implemented by the NTSB Information Security Team as described in the Findings and Recommendations section of this audit report.

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	2	0	0
Improper Usage	0	6	5
Loss or Theft of Equipment	0	1	0
Web	0	0	0
Other	0	0	4
Multiple Attack Vectors	0	0	1
Total	**2**	**7**	**10**

CIO Self-Assessment

The Nuclear Regulatory Commission (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, incident response 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 security events or incidents. The NRC regularly assesses its tool set against the evolving threat landscape and adapts as needed. The NRC rapidly responded 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 reflected in the annual reports provided to OMB and DHS.

Independent Assessment

As the independent assessor the objective was to evaluate the effectiveness of the information security policies, procedures, and practices of the NRC. To achieve this objective, the effectiveness of NRC's information security policies, procedures, and practices on a representative subset of the agency's information systems were evaluated. It was 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. NRC has integrated the Agency's Enterprise Risk Management (ERM) program to address the full spectrum of agency's risk portfolio across all its organizational and business aspect to facilitate the improvement of NRC's mission delivery, reduction of costs, and focus on corrective actions of its key enterprise risks. Additionally, NRC's continuous monitoring program monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM strategy and makes updates to continuously improve its ISCM program. CDM Phase 2 has been completed and CDM Phase 3 is in the process of being implemented. While 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, NRC should strengthen its information security risk management framework by; 1) improving privileged user access reviews and audit log activity, 2) implement an information security architecture across the enterprise, business process, and system levels, 3) integrating system contingency plans and exercises, and 3) Develop and implement privacy role-based training.

FY2020 Annual Cybersecurity Performance Summary

Nuclear Waste Technical Review Board

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		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY18	FY19	FY20
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 FY 2020, the predominate risk to the Nuclear Waste Technical Review Board (NWTRB) was related to the COVID-19 pandemic. The agency has observed an increase in phishing attempts with continued attempts by foreign actors to access cloud-based services. NWTRB updated our remote infrastructure to better support and secure remote access for users teleworking. Phishing awareness training has been given to users with routine reminders being issued throughout the year. The use of vendor-provided services has continued to mitigate the risk of unauthorized access to cloud-based services. Further, NWTRB has continued to maintain sound cyber hygiene practices through regular patching of all information systems. In FY20, NWTRB possessed zero Critical or High vulnerabilities older than seven days on any server or workstation and had no information security, cyber incidents, or breaches., and annual security awareness training was completed for all users to improve awareness and understanding of the importance of security practices. NWTRB continues to prioritize the need for sound cybersecurity practices using assessments to identify areas of strength, improvement, and execution based on those findings.

Independent Assessment

During the period between August 10, 2020 and September 04, 2020, an independent assessor performed an independent security assessment on the Nuclear Waste Technical Review Board's (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 NIST guidelines, FY20 FISMA Metrics, OMB Memorandum M-20-04 and NWTRB Board IT Security Policy requirements.

The security assessment team developed and implemented test procedures to assess stated requirements of the NWTRB SSP. These procedures included visual inspections and reviews/analyses of system documentation. The infrastructure was examined to ensure proper configuration to meet policy requirements. A review of NWTRB system documentation and system configurations was performed to confirm system components were operating as designed and in accordance with policy. The methodology used by the independent assessor consisted of Threat Identification, Vulnerability Identification, Risk Analysis, Corrective Action Recommendation, and Results Documentation.

The independent assessor found that all function areas met or exceeded the Consistently Implemented maturity level. Overall, NWTRB improved its maturity level by increasing maturity in the areas of Identify-Risk Management, Identify-Configuration Management, and Detect-ISCM. Additionally, NWTRB lowered the number of Moderate and Low Risk findings from FY19 and again possessed no High-Risk findings. With consideration of agency risks and constraints, NWTRB will continue to pursue further improvement through the maturity model levels to best protect agency systems.

FY2020 Annual Cybersecurity Performance Summary

Occupational Safety and Health Review Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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

Due to COVID-19, the Occupational Safety and Health Review Commission has moved to a nearly 100% telework environment. Agency deployed image prepared laptops are being used in lieu of Personally Owned Equipment (POE) and fully utilized our COOP situational work program.
Agency realized an expanded use of our cloud-based software agreement and strengthened our security settings on collaboration products.

Independent Assessment

Budgetary funding limits the agency from providing IG services and have engaged with and independent auditor. The independent auditor has worked with the agency to identify their posture with all aspects of the IG metrics requirements in order to provide a assessment of where they are performing as well as areas that require additional resources.
Based on the agencies current efforts the independent auditor deems those efforts as overall effective.
Identify (CA, RA, PM) controls have a rating of Overall Satisfied. Protect (AC, AT, AU, CM, CP, IA, MA, MP, PE, PL, PS, SA, SC, SI) controls have a rating of Overall Satisfied. Detect (IR) controls are rated Overall Satisfied. Respond (controls covered it other areas) controls are Overall Satisfied. Recover (controls covered in other areas) controls Overall Satisfied. This review resulted in 12 remediation items included in the POA&Ms for the agency.

FY2020 Annual Cybersecurity Performance Summary

Office of Government Ethics

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

Incidents by Attack Vector	FY18	FY19	FY20
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

In FY 2020, The Office of Government Ethics (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 2020 FISMA CIO metrics. Twenty-six findings were identified by the assessor, including 15 moderate findings and 11 low findings. Ten of these findings are covered by signed risk acceptances. Five of the existing risk acceptances were "partially met." For those weaknesses, the assessor downgraded the residual risk from "Moderate" to "Low." Consequently, the OGE CIO will write 10 POA&Ms to address outstanding moderate findings. This represents an 80% decrease in the number of POA&Ms compared to the previous assessment. Each finding will be documented, assigned an ID, and monitored until mitigated or accepted by the Authorizing Official (AO). Each POA&M will be signed by the CIO and the AO to indicate either closure or risk acceptance. Also, in FY 2020, OGE engaged with assessors from the Enterprise Services Center to conduct an independent assessment of its information security program using FY 2020 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 second annual audit against these requirements. FY 2019's audit created a solid baseline from which OGE was able to work. FY2020's audit results showed marked improvement, even in the face of challenges placed upon OGE by the COVID-19 pandemic. For purposes of the Audit, the Department of Homeland Security defined five (5) levels of maturity. The high-level result of OGE's FY 2020 IG FISMA Metrics Audit was "Managing Risk" in four out of five levels of maturity, yielding an overall rating of "Managing Risk".

Independent Assessment

The independent auditor found the Office of Government Ethics' (OGE) information security program to be effective. As a micro agency, OGE has a small IT footprint. OGE's systems are actively managed by a small, skilled Federal staff, dedicated to maintaining the confidentiality, integrity and availability of their systems. OGE still has opportunities for further improvement in each of the Domains; however, OGE personnel made significant progress during FY20 following FY19's IG FISMA Metrics Audit.

FY2020 Annual Cybersecurity Performance Summary

Office of Navajo and Hopi Indian Relocation

Framework	CIO Rating	IG Rating
Identify	At 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	FY18	FY19	FY20
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

Several updates, fixes, installs, and patches were completed to help mitigate cybersecurity risks to the Agency. Our network team had been working on getting the new computer equipment ready to accept PIV card information and staff needed to make appointments to update their PIV cards and complete training on the use of their PIV cards. The Agency also procured software so those staff that signed into our server would use multifactor factor authentication and training was made available to staff on its use for access. Different spam software needed to be researched as the current spam software went out of business. More training on phishing found in emails and a phishing hook icon was installed in all staff's Microsoft Office 365 outlook software. The network team had to halt some work in order to complete incoming BOD's or ED's. The Agency needed to procure more iPhones so that staff who stayed home during this COVID-19 period could check on e-mails. We then completed the project of installing MDM software on all staff iPhones. All the above projects have been completed and at this time we do not use telework, as essential staff have their own office to complete needed work. As part of our normal yearly audit in FY17, the independent auditor reviewed our department and never recommended further changes. For FY18 and FY19 the DOI has procured an audit of our Agency and we hope to be closed by end of calendar year.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Office of Navajo and Hopi Indian Relocation was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the Agency shall engage with an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

Office of Personnel Management

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	4	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	123	156	167
Loss or Theft of Equipment	8	10	9
Web	1	0	0
Other	28	57	32
Multiple Attack Vectors	0	1	0
Total	**160**	**228**	**208**

CIO Self-Assessment

The agency has continued our efforts to enhance our cybersecurity posture and infrastructure through technology modernization, as well as policy and procedure updates. Significant improvements were made through widespread device replacements, reducing, and in some cases, eliminating unsupported operating systems in our environment. These ongoing modernization initiatives created a more secure and smooth pivot to telework at the Office of Personnel Management (OPM). Additionally, our security training strategy and program is rated by our OIG as Level 4 - Managed and Measurable through our efforts to effectively and consistently provide meaningful training to OPM employees. The agency Risk Management Council and associated risk management strategy continue to mature and further growth is planned for FY 2021.

Independent Assessment

The FY 2020 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 eight “domains” under the function areas. These eight 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 evaluate and test when assessing the agency’s cybersecurity program. Each metric receives a maturity level rating of 1-5.

The mode (i.e., the number that appears most often) from the maturity levels of each individual metric is used to determine the corresponding domain rating and in the event of a tie between maturity levels the higher level is used. Similarly, the mode from the domain ratings assigns the function area rating. We calculated the overall agency rating using the same methodology. However, IGs have discretion in the function and agency ratings to consider agency specific factors.

In FY 2020, OPM's cybersecurity maturity level is measured as 2 - Defined.

Level 4, Managed and Measurable, is an effective level of security at the domain, function, and overall program level. Therefore, the information security program is deemed ineffective. Recommendations have been provided for metrics defined as ineffective to assist in elevating the program's overall level. These recommendations can be found in the comments sections for specific metrics.

FY2020 Annual Cybersecurity Performance Summary

Office of Special Counsel

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	2	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**	**2**	**0**

CIO Self-Assessment

The Office of Special Counsel (OSC) IT staff reviewed its cybersecurity risk management program, and invested in evolving and maturing a risk-based and cost-effective cybersecurity program. In FY 2020 as a small IT Team, OSC looked for tools to add to the environment that would integrate with the existing network architecture. Taking the cloud-first approach, OSC was able to enhance its security by implementing cloud-based vulnerability and risk scanning and mitigation tools. OSC also deployed an Endpoint Configuration Manager for configuration and compliance in a Hybrid architecture allowing an enterprise-wide management from a single source. These on-premise and cloud systems were tied together through a new single security information and event management (SIEM) collection and analysis portal. OSC also deployed conditional access and cloud app security to enhance data protection and further secure access to the OSC network. OSC also completed its evaluation for a TIC 3.0 compliant secure access service edge for all OSC endpoints with an aim of immediate wide-scale adoption. OSC is committed to further strengthening and enhancing the Cybersecurity Program in the upcoming fiscal year.

Independent Assessment

DOI Information Systems Security line of Business (ISSLoB) performed an assessment of the current implementation of the OSC GSS. OSC underwent a security assessment from 06/2020 to 10/2020 based on FY 2020 IG FISMA Reporting Metrics provided by DHS and OMB. During this period of time, ISSLoB interacted with OSC personnel and reviewed evidence and artifacts in order to assess the implementation of the OSC GSS.

Upon completion of the audit, it is apparent that OSC continues to work towards improving the level of security within the organization’s GSS environment. OSC has complied with most security control requirements tested during the security assessment of OSC’s 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:

- Vulnerability scanning of agency information systems and assets has been established and is performed according to FISMA security requirements;
- OSC has established an effective configuration management program for its information systems and major applications by employing the use of automated mechanisms that provide on-demand and real-time baseline, security configuration requirements, and risks views of the entire agency infrastructure;
- State of the art automated mechanisms are employed to support FISMA requirements for the Risk Management, Access Control, and ISCM programs; and,
- OSC ensures that basic and specialized Security Training is monitored and provided to OSC stakeholders at least annually and given to OSC personnel according job functions and levels of access;

FY2020 Annual Cybersecurity 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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	13	0	0
External/Removable Media	0	0	0
Impersonation	1	0	0
Improper Usage	0	10	5
Loss or Theft of Equipment	8	0	0
Web	0	0	0
Other	7	3	0
Multiple Attack Vectors	0	0	0
Total	**29**	**13**	**5**

CIO Self-Assessment

The OCC's approach to reducing and managing risks associated with expanded telework include:

- leveraging its endpoint controls for signature-based threat detection and prevention;
- malware quarantining, upload and copy/paste off-network prevention, and cloud-based vulnerability scanning and reporting;
- hardware-based white- and black-listing to improve workforce security both on and off the OCC network;
- communicating regularly with its workforce regarding agency-supported collaboration tools;
- establishing clear restrictions on the use of commercial video teleconferencing services;
- continuing weekly phishing exercises to increase end user awareness, with improved reporting to enable outreach and education through supervisory chains;
- expanding its monitoring and log review capabilities to detect and eliminate threats.

Independent Assessment

For the FY 2020 FISMA Unclassified performance audit, the independent auditor assessed the effectiveness of OCC's bureau-level information security controls that align to the FY 2020 IG FISMA Reporting Metrics for the period July 1, 2019 through June 30, 2020. Where relevant, the assessor tested these in-scope information security controls for Financial Management External Service Providers and Managed Disaster Recovery Solution. 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 2020 performance audit.

FY2020 Annual Cybersecurity Performance Summary

Peace Corps

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	19	13	13
Loss or Theft of Equipment	1	0	0
Web	0	0	0
Other	5	8	8
Multiple Attack Vectors	0	0	0
Total	**25**	**21**	**21**

CIO Self-Assessment

Our assessment reflects that the Peace Corps lacks an effective information security program, as the Department of Homeland Security considers Level 4, Managed and Measurable, to be an effective level of security for the overall program. Based on the assessment of the Peace Corps' information security program, the overall maturity level results are in between Level 1, Ad-hoc, and Level 2, Defined. As such, we identified issues relating to the people, processes, technology, and culture aspects across all the Cybersecurity Framework Function areas. In order to address some of those issues and advance the information security program, the Agency has augmented its cybersecurity staff resources for FY 2021-2022. In FY2020, technical improvements, like implementation of CDM, EINSTEIN and a more robust disaster recovery solution were made to improve our identify, detect, and recovery functions. Finally, in order to mitigate risks like COVID-19, Peace Corps fully migrated to a more secure, distributed VPN solution, removed split tunneling for end-user devices and removed Windows 7 from the environment.

Independent Assessment

Our assessment reflects that the Peace Corps lacks an effective information security program, as the Department of Homeland Security considers Level 4, Managed and Measurable, to be an effective level of security for the overall program. Based on the assessment of the Peace Corps' information security program, the overall maturity level results are in between Level 1, Ad-hoc, and Level 2, Defined. As such, we identified issues relating to the people, processes, technology, and culture aspects across all the Cybersecurity Framework Function areas. Moving forward, to advance and fully develop the information security program, involvement from all levels of the Peace Corps leadership is needed.

FY2020 Annual Cybersecurity Performance Summary

Pension Benefit Guaranty Corporation

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	1	3	2
Loss or Theft of Equipment	0	0	0
Web	0	0	0
Other	0	1	0
Multiple Attack Vectors	0	0	0
Total	**1**	**4**	**2**

CIO Self-Assessment

The Pension Benefit Guaranty Corporation (PBGC) s responsible for protecting both the pension benefits and data privacy of plan participants. Protecting PBGC networks, systems, and data is a long-standing and continuing management challenge. Thus, data protection continues to be a priority given the high volume of personally identifiable information in PBGC’s possession. In addition, security domains within the CSF functions falling short of the “effective” threshold per fiscal year OIG FISMA audit engagements, remain challenges and potential risks. Further improvements in PBGC’s information security posture are needed so that the Corporation can remain agile in the rapidly changing threat environment. Management has recognized these challenges and will continue to work collaboratively with the PBGC Office of Inspector General (OIG). In the past fiscal year, cybersecurity risks have been mitigated and security and privacy controls have been strengthened due to enhanced compliance and oversight. PBGC managed identified risks by developing and implementing risk mitigation plans, creating POA&Ms, and accepting risks where operational constraints exist. Additionally, programmatic strategies and approaches were employed that ensured PBGC systems are compliant with the Corporation’s Information Security Program and applicable laws and regulations. PBGC continued to mature its enterprise risk management practices and improved risk-based prioritization of its resources by briefing executives from each business unit about cybersecurity risks impacting their programs. The CIO continued to sponsor the PBGC Cybersecurity and Privacy Council comprised of Federal Information System Security Managers from the Corporation’s business units with the goal of sharing information and making recommendations pertaining to cybersecurity and privacy.

Independent Assessment

The 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 2020 IG FISMA metrics under OIG oversight.

In FY 2020, the independent auditor reviewed a sample of eight systems. The independent auditor noted improvements in 34 metrics throughout the eight domains. PBGC raised the maturity of the configuration management and security training domains to managed and measurable. However, PBGC’s overall IT security program was rated as not effective as three of the five functions were still rated at Consistently Implemented.

Our detailed report and recommendations will be available in our audit report of PBGC's FY 2020 compliance with FISMA.

FY2020 Annual Cybersecurity Performance Summary

Postal Regulatory Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
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

During this past year, the Postal Regulatory Commission (the Commission) has taken steps to improve the overall security and performance of its systems and IT Infrastructure. The Commission hired a new Cybersecurity Manager who immediately initiated a Security Assessment of the General Support System. Once the assessment is complete, the Commission will prioritize and address any security findings specifically focusing on high-risk areas of concern and take the appropriate steps to improve the Commission's security program. In addition, we continue to collaborate with the Department of Homeland Security (DHS) utilizing the Continuous Diagnostics and Mitigation (CDM) program to identify and address risks, and other security programs such as Einstein 3(a) and Managed Trusted Internet Protocol Service (MTIPS), allowing the Commission to improve its cybersecurity posture. With new security threats continually emerging, the Commission continues to enhance its security practices and policies to better protect sensitive information and to educate employees about the importance of safeguarding the Commission's IT Infrastructure, applications, and data.

Independent Assessment

The Postal Regulatory Commission's Office of the Inspector General (OIG) was established in June 2007, as required by an amendment to the Inspector General Act of 1978 included in the Postal Accountability and Enhancement Act of 2006 (Public Law 109-435 sec. 605). The Commission's OIG operates independently of the Commission and the Commission does not control whether the OIG conducts an independent evaluation of the status of the IT cybersecurity program.

FY2020 Annual Cybersecurity Performance Summary

Presidio Trust

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	3	3
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	0	0
Loss or Theft of Equipment	0	1	3
Web	0	0	0
Other	0	1	1
Multiple Attack Vectors	0	0	0
Total	**0**	**5**	**7**

CIO Self-Assessment

The Presidio Trust (The Trust) is a small, government-owned corporation that has unique mandates under the Presidio Trust Act for Property and Fiscal Management. The Trust's security program goals focus on reducing cybersecurity risk which could affect the confidentiality of personal information of tenants and staff, integrity of the agency's property management and financial data, and availability of technology systems supporting our mission while aligning with federal guidance for agency security programs. The Trust continues to evaluate and reduce risk, whether it originates externally or internally, from natural disasters, accidental or intentional events. In FY20, the Trust has made considerable progress in several foundational areas to reduce risk:

- Developed business continuity plans specific to every division of the agency
- Deployed new collaboration tools and VPN infrastructure to enable secure remote work
- Implemented a data loss prevention program
- Trained all employees, contractors and members of the Board of Directors in security
- Revamped our onboarding and offboarding processes

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the Presidio Trust was not performed for FY 2020, and the IG assessment section is marked "Not Applicable" (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

Privacy and Civil Liberties Oversight Board

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		Managed and Measurable
Overall	**Managing Risk**	

Incidents by Attack Vector	FY18	FY19	FY20
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 significant progress towards implementing NIST controls to mitigate risks to IT assets, environment, and mission-critical functions from cyber attacks. The Board implemented additional solutions and controls to support telework users in response to COVID-19. The FY 2020 independent audit validated the Board's efforts rating the PCLOB controls as effective. The independent audit identified four controls for remediation. The Board also achieved Full compliance with DHS EDs and BODs 20-02, 20-03, and 20-04 and suffered no major information security incidents in FY 2020.

Additionally, the Board enhanced 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 leverage 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 2020 independent audit identified four findings for selected controls. The PCLOB has develop POAM's to remediate the auditor's findings. PCLOB had no findings for FY 2019 and successfully closed eighty-five percent of FY 2018 findings. The PLCOB also commissioned an independent vulnerability assessment of its IT infrastructure 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.

FY2020 Annual Cybersecurity Performance Summary

Railroad Retirement Board

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	23	21	10
Loss or Theft of Equipment	24	18	16
Web	0	0	0
Other	4	20	0
Multiple Attack Vectors	0	0	0
Total	**51**	**59**	**26**

CIO Self-Assessment

The adequacy and effectiveness of the Railroad Retirement Board's (RRB) information security policies, procedures, and practices is progressing as directed by OMB, DHS, NSC staff, and the CIO Council and is reflected in the RRB's IG FY 2020 metric report.

Recognizing that our cybersecurity program is continuing to improve, the CIO and CISO acknowledge the cybersecurity risks identified in the FY 2020 FISMA audit conducted by the RRB's OIG. Our goal is to remediate those cybersecurity risks as soon as possible.

Fiscal Year 2020 was very challenging to manage the RRB cybersecurity program during the COVID-19 pandemic. The CIO and CISO addressed the following concerns:

1. Flaw Remediation - We had to develop a patch management program that still remediate vulnerabilities while consider bandwidth concerns when all of the RRB employees worked remotely. A plan was developed and the RRB is maintaining a strong risk tolerant posture.
2. Asset Management - The RRB continues to work through gaps in our hardware assessment management program. The CISO, enrolled in the DHS CDM Defend program is addressing those issues.
3. IT Modernization - The CIO's vision for IT Modernization continues to move forward. A plan to migrate the on-premise mainframe to the cloud is in place and a plan to modernize the current RRB applications is being conducted by GSA 18F.

Independent Assessment

To assess how the RRB established and implemented its agency-wide Information Security Program and practices, as required by FISMA, our independent auditor performed detailed testing of 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 NIST SP 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations. Overall, the Information Security Program was rated ineffective. Continued management attention is necessary in all functions, as the independent auditor identified that RRB scored below the "managed and measurable" level in multiple security metrics within all functions.

FY2020 Annual Cybersecurity Performance Summary

Securities and Exchange Commission

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	1	0
E-mail	339	249	13
External/Removable Media	0	0	1
Impersonation	0	0	0
Improper Usage	100	57	37
Loss or Theft of Equipment	1	0	0
Web	36	24	2
Other	74	61	5
Multiple Attack Vectors	2	4	0
Total	**552**	**396**	**58**

CIO Self-Assessment

During FY 2020, the Securities and Exchange Commission (SEC) continued to make progress toward improving its information security program amidst challenges presented by the COVID-19 pandemic. The SEC increased anti-phishing and other awareness training efforts, improved security vulnerability mitigation capabilities, enhanced its continuous monitoring program, and further improved incident detection and management capabilities.

The SEC conducted quarterly phishing exercises for all employees and contractors. Personnel, identified by exercises as being susceptible to phishing, were required to undergo supplemental training. A vulnerability disclosure policy and submission process were established to encourage independent security researchers to report potential vulnerabilities they discover in SEC systems before publicly disclosing their research. Multiple third parties, including DHS, conducted penetration testing, architecture reviews, and other risk assessment activities to identify vulnerabilities and test incident response mechanisms. Capabilities for detecting and preventing software and website vulnerabilities were enhanced by implementing new vulnerability assessment tools and conducting proactive source code reviews.

The NIST Cybersecurity Framework was used to complete risk profiles for all the SEC's HVA systems. The SEC's Office of Information Technology (OIT), in partnership with business owners, completed security assessment and authorization activities for 67 FISMA reportable systems. OIT also facilitated the remediation of over 425 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 enough to close seventeen prior-year IT related OIG audit recommendations and two IT related GAO audit recommendations.

Independent Assessment

Despite facing unique challenges presented by COVID-19, including a significant increase in telework, the SEC has made progress in improving its information security program by refining its risk management tools, initiating processes to develop a software asset and license inventory, improving the timeliness of security patch deployments, enhancing its security awareness and training processes, continuing its efforts to enhance its continuous monitoring program, and improving its incident response capabilities.

While the SEC made program improvements, the Agency continued to face challenges with developing a supply chain management action plan, fully implementing its software asset management solution, relating hardware scanning tools and technologies via a standard taxonomy, enforcing strong authentication mechanisms, enhancing its configuration management activities, and delivering specialized security training. As a result, an independent assessor determined that the SEC's information security program did not meet the definition of "effective."

FY2020 Annual Cybersecurity 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	Consistently Implemented
Recover		Managed and Measurable
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
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 OCIO has driven significant IT Modernization accomplishments in FY2020 that have resulted in a substantial reduction in cyber risks while increasing capacity and service to the Agency's Network/System's resiliency of circuity connections and disaster recovery in support of COOP. The 2020 modernization initiative started at the Arlington Headquarters and continued at the Chicago Data Management Center (DMC). The completion of the GSA EIS contract award to an ISP led to the upgrade of all the Agency MTIPS/MPLS Circuits that has substantially improved service while strengthening cybersecurity throughout the Enterprise. Additionally, the redundant 1GB MPLS connections from Arlington to Chicago allow for the "Round Robin" load balancing of our new VPN service to the agency. This 2020 VPN service improvement has proved an operational mission changer for the Agency's success in the era of the COVID-19 national emergency.

Independent Assessment

The OCIO and CISO acknowledge the 2020 FISMA Audit NFR. The OCIO remains committed to the closure and sustainment of all Cyber Security Compliance requirements through engaged OCIO/CISO governance. The CIO will ensure compliance with each audit recommendation by actively working to close all existing remediation's and Corrective Action Plans (CAPs) with a continued sense of measured urgency and transparency on the documented dates of CAP completion. The OCIO will ensure compliance with OMB A-50 and all Federal regulations to ensure SSS IT/Cyber operations achieves or sustains the highest compliance standards in the Federal Government.

The new Deputy CIO and CISO will be assigned co-responsibility for continual compliance and governance with the performance expectations through monthly briefs to the CIO and Agency Leadership of the status of CAPs as a standing agenda item in the Monthly Configuration Control Board (CCB).

Additionally, the CIO has approved the acquisition of the Department of Justice's 'Cyber Security Assessment and Management' (CSAM) application for the effective management of Critical Vulnerability and Exposures (CVE) POA&M tracking and remediation; as well as serving as a mature application for the development and certification of Internal Use Software and Network/Cloud Accreditation Packages.

The OCIO is committed timely oversight, compliance, and closure of all findings with rigorous CAPs and will govern under the overarching HQ Order 20-03 for the Correction of Audit Findings and Recommendations to maintain compliance with OMB Circular A-50 's requirements the development of CAPs in response to audit, GAO, IG, and other reports.

FY2020 Annual Cybersecurity Performance Summary

Small Business Administration

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	1	4	43
E-mail	135	1,100	1,694
External/Removable Media	0	6	0
Impersonation	0	7	37
Improper Usage	45	134	494
Loss or Theft of Equipment	16	6	7
Web	19	139	415
Other	128	368	238
Multiple Attack Vectors	0	1	1
Total	**344**	**1,765**	**2,929**

CIO Self-Assessment

During FY 2020, the Small Business Administration (SBA) further operationalized its cybersecurity strategy, establishing direction and priorities for cybersecurity across the agency. The SBA continued in its implementation and maturation of Enterprise Cybersecurity Services (ECS), with the ultimate goals of full visibility, consistency of process, rapid response, and resiliency. Focus areas included expansion of Cyber Threat Intelligence (CTI), increased adoption of strong authentication, continued migration to cloud-based solutions, and emphasis on continuous monitoring.

The SBA continued building a robust, adaptable, and cost-effective cybersecurity program thus strengthening the overall security posture of agency IT systems during SBA's CARES ACT implementation and COVID-19 response. The SBA realized significant cost savings and cost avoidance through integration of agency systems into its enterprise cybersecurity services by eliminating duplicative and unnecessary tools. Finally, the SBA tailored its RMF control baseline, eliminating redundant controls, as a leap towards our Ongoing Authorization goals.

Independent Assessment

The information security program of the Small Business Administration (SBA) was evaluated as not effective. Consistent with applicable FISMA requirements, 0MB policy and guidelines, and NIST standards and guidelines, OIG evaluated the design, implementation, and operating effectiveness of SBA's information security policies, procedures, and practices. OIG determined that SBA has established and maintained its information security program and practices for the eight FISMA metric domains. SBA maintained the rating of its incident response program to as "Managed and Measurable" and is operating in an effective manner. SBA's identify and access management program also went from "Defined" to "Consistently Implemented". However, other than the incident response program, the other seven domains of the program reflected deficiencies that we identified were not fully effective. SBA has worked to implement recommendations from previous FISMA reports. While the OIG acknowledges the impact the COVID pandemic and subsequent CARES Act processing requirements greatly challenged the security posture of SBA, we also recognize challenges remain in implementing an effective IT security program for the agency.

FY2020 Annual Cybersecurity Performance Summary

Social Security Administration

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	FY18	FY19	FY20
Attrition	66	267	241
E-mail	67	90	42
External/Removable Media	0	5	3
Impersonation	2	13	43
Improper Usage	1,547	1,462	2,386
Loss or Theft of Equipment	38	35	41
Web	501	560	1,800
Other	1,147	2,353	4,305
Multiple Attack Vectors	1	11	17
Total	**3,369**	**4,796**	**8,878**

CIO Self-Assessment

The Social Security Administration's (SSA) mission requires it to collect PII for over 325 million Americans. This information is vital to performing the SSA's essential functions, but makes its network, systems, and databases a rich target for adversaries. In FY 2020, we increased emphasis on governance and oversight in cyber at the enterprise level by further engaging leaders from components outside IT, creating greater awareness of risks, and establishing more accountability for program objectives and milestones. Specifically, in the Identify area of the NIST CSF, we:

- Applied our RMF strategy to rank risks stemming from audits and security risk assessments;
- We progressed toward our goal of implementing a Configuration Management Database (CMDB) to enhance SSA's hardware, software, and system inventories;
- We continued to enhance our abilities to identify, detect, and remediate vulnerabilities through continuous vulnerability scanning, testing based on DHS' AWARE scoring;
- We created Executive risk dashboards to enhance visibility into our security posture.

In the Protect area, we

- Strengthened our protection of high value assets;
- Strengthened our configuration management by isolating non-compliant hardware and software from our network; and
- Strengthened our defenses for Data Loss Protection and Intrusion Detection and Prevention.

In the Detect area, we revamped our information security continuous monitoring strategy to incorporate changes to process and technology, DHS' Continuous Diagnostic and Mitigation program (CDM) capabilities to make informed risk-based decisions.

In the Respond area, we improved our Agency incident response plan and achieved Level 4 maturity rating from our independent auditor indicating operational effectiveness.

In the Recover area, we published new guidance related to continuity of business operations via updates to our Administrative Instructions Manual System guide as well as our new Emergency Management Handbook

Independent Assessment

Although SSA established an agency-wide information security program and practices, our Independent Public Accountant (IPA) identified deficiencies related to:

- Risk management;
- Configuration management;
- Identity and access management;
- Data protection and privacy;
- Security training;
- Information security;
- Continuous monitoring;

FY2020 Annual Cybersecurity Performance Summary

Surface Transportation Board

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

Incidents by Attack Vector	FY18	FY19	FY20
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	8
Multiple Attack Vectors	0	0	0
Total	**0**	**0**	**8**

CIO Self-Assessment

The Surface Transportation Board (STB) is in its third year of improvement and maturation of its cybersecurity posture. 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 appreciates that this year's audit recognizes the work that has been done through FY 2020 while providing the STB with a roadmap for continued improvements.

In addition to the improvement of various cybersecurity related processes, the STB developed and implemented an organizational privacy program that addresses many security controls of NIST SP 800-53 Revision 4.

Independent Assessment

For the FY 2020 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. The FY 2020 audit covered the period from October 1, 2019 to May 31, 2020. 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, six (6) recommendations were closed and two (2) remain open at the conclusion of the FY 2020 audit. Furthermore, DOT OIG independent assessor issued six (6) new recommendations to support STB's efforts to define and implement its information security program and processes. At the conclusion of the FY 2020 audit, STB's information security program was rated at a Level 2, Defined.

FY2020 Annual Cybersecurity 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	Consistently Implemented
Respond	Managing Risk	Managed and Measurable
Recover		Consistently Implemented
Overall	Managing Risk	

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	1	0	2
External/Removable Media	0	0	1
Impersonation	1	1	0
Improper Usage	7	2	3
Loss or Theft of Equipment	17	4	14
Web	0	0	0
Other	2	15	1
Multiple Attack Vectors	0	1	0
Total	**28**	**23**	**21**

CIO Self-Assessment

In March, the Tennessee Valley Authority (TVA) reacted to the COVID-19 pandemic and implemented teleworking across the Agency to maintain continuity of operations. TVA leveraged existing VPN and multi-factor authentication technology to maintain a controlled environment. Additionally, TVA emphasized its remote access best practices for the workforce. TVA leveraged the existing teleconference platform and emphasized to employees that the use of other teleconference applications is not permitted. Contingency plans were solidified to ensure capacity was stable as remote work increased. TVA increased the use of virtual desktops and cloud applications so personnel could access information remotely. TVA increased connection visibility and strengthened monitoring across the cloud implementations and internal networks. TVA continued to educate and test employees through its phishing program, allowing TVA to remain focused on promoting and reinforcing acceptable user behavior. TVA also includes warning banners on e-mails originating from outside of the corporate infrastructure, encouraging users to treat these e-mails with heightened awareness. As part of TVA's intentional communication to employees, websites for obtaining COVID information were shared. TVA conducted a study on its network architecture with the goal of moving to a zero-trust model and closing security and resiliency gaps. Patching end point systems was moved to the cloud to ensure all patches are applied in a timely manner. A strong geolocation blocking standard was implemented and enforced. TVA continues to comply with DHS-developed directives as required by Title 44 USC, Chapter 35, Section 3553. TVA operates an effective information security program and will continue to use a risk-based approach to prioritize security maturity and make appropriate investments in order to protect its mission and operations.

Independent Assessment

Based on the analysis of the metrics and associated maturity levels defined by FY 2020 IG FISMA metrics, we found TVA’s information security program was operating in an effective manner. In addition, analysis of the Identify and Detect Functions resulted in improvements 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 2020 IG FISMA metrics.

FY2020 Annual Cybersecurity Performance Summary

U.S. International Development Finance Corporation

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	FY18	FY19	FY20
Attrition	0	0	0
E-mail	2	0	1
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	0	1	0
Loss or Theft of Equipment	9	10	5
Web	0	0	0
Other	2	0	2
Multiple Attack Vectors	0	0	0
Total	**13**	**11**	**8**

CIO Self-Assessment

While DFC does not have High Value Assets (HVA), the Agency has determined that the greatest cybersecurity risks are the untimely remediation of hardware and software vulnerabilities, incomplete implementation of multi-factor authentication (MFA) for privileged accounts and for access to O365, as well as lack of detection of unauthorized assets. To mitigate the risk of untimely remediation of hardware and software vulnerabilities, DFC has developed and implemented five main customized processes for patching varying types of vulnerabilities based on their severity levels, degree of deviation, and/or status during out-of-cycle patch scheduling. In parallel, the Agency has invested in, and installed, an enterprise-wide vulnerability management solution to automate the majority of needed patches DFC identifies through robust routine scans of its network assets. To address the incomplete implementation of MFA, DFC has developed a plan to enforce MFA on all privileged user accounts and for all O365 access vectors as part of the Agency's infrastructure upgrade. Meanwhile, DFC continues to implement MFA to both on-site and remote network access, perform detailed and periodic account reviews, and train users to identify malicious emails designed to obtain network credentials. The Agency is also in the process of modifying its password policy, which would require network account users to select even stronger passwords in alignment with NIST guidance. To mitigate the risk of unauthorized assets, DFC locks down network access points and collaborates with third-party vendors to determine automated methods for detecting the use of rogue hardware and software on the Agency's network.

Independent Assessment

DFC's information security program was evaluated as part of the FY2020 FISMA Audit. This audit included an evaluation of the entire population of three FISMA reportable systems at DFC. The FY2020 FISMA Audit noted 66 of 75 selected NIST SP 800-53, Revision 4 security controls were properly implemented. 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 FY2020 FISMA Audit report.

FY2020 Annual Cybersecurity Performance Summary

U.S. Trade and Development Agency

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

Incidents by Attack Vector	FY18	FY19	FY20
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	1	0	0
Multiple Attack Vectors	0	0	0
Total	**2**	**0**	**0**

CIO Self-Assessment

The U.S. Trade and Development Agency (USTDA) has continuously improve and enhance the security of our information services. USTDA has completed its transition from the TIC/MTIPS to the new GSA EIS requirement and has been operational since September 30, 2020, as well as secured additional resources and tools to be implemented that would allow USTDA to have a stronger security posture.
We completed an IT hardware technology refresh for all agency users that allowed the agency a seamless transition to mandatory telework mode during COVID-19. The implementation of PIV for logical laptop authentication and digital signing was completed. We are also on course to transform its overall IT collaboration platform to SharePoint online, which will result in streamlined workflows and better records management. These efforts will support NARA requirements.

Independent Assessment

While only two of the five ratings in the function areas are Managed and Measurable or above, the two ad-hoc ratings are based on the need for formal procedures. While implemented practices support the intended functions, the formal procedures remain to be finalized and approved. For this reason, the overall rating was adjusted to effective.

FY2020 Annual Cybersecurity Performance Summary

United States AbilityOne Commission

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	FY18	FY19	FY20
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	1	0
Web	0	0	0
Other	0	0	0
Multiple Attack Vectors	0	0	0
Total	**0**	**1**	**0**

CIO Self-Assessment

The Commission encountered minimum risk during this period. No additional controls were required because we were a partial telework agency prior to COVID-19. In light of COVID-19, the Commission implemented its COOP and transitioned to full telework from March 2020 until the present. Our risk was minimized by remotely accessing our internal resources via VPN access. Next, monitoring was increased in order to detect any rouge connection. Finally, the Commission reached out to FedRAMP to meet and collaborate.

Independent Assessment

The objective of the evaluation was to assess the effectiveness of the Commission's security program and practices across key functional areas as of September 30, 2020. The Commission made progress through implementation of security policies, procedures, and strategies, but lacked quantitative and qualitative measures to assess them. During FY20, there were six findings and nine corresponding recommendations regarding the Commission's information security program. The overall assessment of the Commission's FY2020 information security program was deemed effective because the tested, calculated and assessed maturity levels across the functional and domain areas received an overall rating of effective. The Commission implemented the three open prior year recommendations and OIG provides nine new recommendations corresponding to six new findings.

FY2020 Annual Cybersecurity Performance Summary

United States Access Board

Framework	CIO Rating	IG Rating
Identify	At 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	FY18	FY19	FY20
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 United States Access Board (USAB) has strengthened their information security policies and processes by identifying gaps in their security posture. The agency has taken an overall risk assessment approach while in preparation for ATO. The agency has created a POA&M to address those gaps.

During FY 2020, USAB has improved the security of their environment by implementing strict telework policies and standard operating procedures during the COVID-19 pandemic. USAB plans to implement TIC 3.0 to focus on improving their cybersecurity strategy, architecture, and visibility in the upcoming FY 2021.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the United States Access Board was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.

FY2020 Annual Cybersecurity Performance Summary

United States Agency for Global Media

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

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	0
E-mail	2	2	1
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	4
Multiple Attack Vectors	0	0	0
Total	**5**	**8**	**5**

CIO Self-Assessment

The United States Agency for Global Media (the Agency)'s pandemic response greatly increased the number of our employees who were teleworking, and the quantity of hours they were teleworking. Currently, almost 99 percent of our agency's staff and contractors do all of their work remotely. This has posed a serious risk to our IT security program, since a significant portion of our IT security defenses, prior to the pandemic response were centered on protecting our internal network and the devices connected to it. To mitigate this, our Operational Security team quickly deployed new security tools. These new tools have proven instrumental in keeping our Agency remote computers and users safe from malicious attacks during the pandemic.

Independent Assessment

The U.S. Agency for Global Media information security program was evaluated by an independent contractor against FISMA requirements in FY 2020. The assessment scope included a selection of USAGM's major information systems. OIG's independent contractor found that USAGM generally implemented pieces of an information security program that supports the operations and assets of USAGM. However, the assessment identified numerous areas where policies were not current and where controls and processes could be improved. The independent contractor concluded that USAGM does not have an effective organization-wide information security program. The assessment resulted in 22 recommendations with identified weaknesses across most domains and all functional areas.

FY2020 Annual Cybersecurity 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		Consistently Implemented
Overall	Managing Risk	

CIO Self-Assessment

Despite the challenges presented by the COVID-19 pandemic, the U.S. Agency for International Development (USAID) successfully pivoted our entire enterprise, literally overnight, to a safe and productive telework environment as a direct result of the our decade of IT modernization and investments in cloud technologies.

USAID is a leader in the Federal Government leader in adopting cloud computing. Our cloud collaboration platform enabled the enterprise to increase our computing capacity quickly and accommodate bursts in usage by implementing elastic provisioning and bandwidth-on-demand.

The Agency was able to leverage modernized and streamlined communications by using our audio/video collaboration tools for the workforce (all approved by FedRAMP).

Additionally, the Agency rapidly rolled out upgraded firewalls across the enterprise expanded remote patching capabilities; stepped up education and awareness campaigns on cyber threats for our workforce; and expanded the use of management and oversight tools, such as the automated portions of the FISMA Continuous Monitoring Executive Dashboard created by the OCIO in the Bureau for Management to track vulnerabilities in our IT systems. As a result of these actions and investments, USAID was able to mitigate cybersecurity risks to the Agency's network, data, and workforce while continuing to deliver on our mission in more than 80 countries around the world despite the challenges of addressing a more than 400-percent increase in cyber incidents spawned by the pandemic.

Incidents by Attack Vector	FY18	FY19	FY20
Attrition	0	0	1
E-mail	2	6	2
External/Removable Media	0	3	1
Impersonation	2	0	0
Improper Usage	15	22	37
Loss or Theft of Equipment	9	3	3
Web	8	24	46
Other	20	103	65
Multiple Attack Vectors	0	1	2
Total	**56**	**162**	**157**

Independent Assessment

USAID's information security program was evaluated as part of the FY 2020 FISMA Audit. This audit included an evaluation of 6 out of 58 FISMA reportable systems at USAID. The FY 2020 FISMA Audit noted 123 of 135 selected NIST SP 800-53, Revision 4 security controls were properly implemented. This led to the determination of USAID having an overall effective information security program. There were 7 recommendations made to help USAID improve their information security program. These recommendations can be found in the FY 2020 FISMA Audit report.

FY2020 Annual Cybersecurity Performance Summary

United States Interagency Council on Homelessness

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

Incidents by Attack Vector	FY18	FY19	FY20
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

Per NIST FIPS 199 Categorization, USICH's sole information is categorized as Low Impact. For FY 2020, USICH continued to work with its IT service providers in ensuring IT compliance by updating and revising its systems as necessary. USICH's SSP plan will continue to support compliance and be updated as necessary.

Independent Assessment

An independent evaluation of the status of the IT cybersecurity program for the United States Interagency Council for Homelessness was not performed for FY 2020, and the IG assessment section is marked “Not Applicable” (NA). Per FISMA, Sec. 3555(b)(2), where agencies do not have an OIG appointed under the Inspectors General Act of 1978, the head of the agency shall engage an independent external auditor to perform the assessment.