FY2022 Annual Cybersecurity Performance Summary

United States Agency for International Development (USAID)

Framework	CIO Rating	IGRating
Identify	15	Defined
Protect	34	Managed and Measurable
Detect	5	Managed and Measurable
Respond	15	Optimized
Recover	15	Managed and Measurable
Overall	84%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	1	2
E-mail	2	10	2
External/Removable Media	1	2	0
Impersonation	0	0	0
Improper Usage	37	30	37
Loss or Theft of Equipment	3	0	0
Web	46	14	27
Other	65	60	57
Multiple Attack Vectors	2	2	0
Total	157	119	125

CIO Self-Assessment

In FY 2022 the USG experienced ongoing data breaches and compromises from our strongest adversaries, resulting in numerous government actions and Emergency Directives (ED). It is critical that USAID continue to develop and execute a robust cyber response playbook that anticipates, adapts to, and mitigates threats to our workforce and Agency mission delivery. USAID remains committed to prioritizing critical services and technologies to modernize the Agency and comply with Executive Order (E.O.) 14028, as well as aligning with the cybersecurity priorities set forth in the President's Management Agenda, Priority 3 - Strategy 2 section, and other cyber directives and mandates. For example, in FY 2022, USAID continued to educate the global workforce by:
•expanding its cyber awareness campaign;
•issuing numerous Cybersecurity and Privacy notices and alerts; and
•continuing the Anti-Phishing program that involves sending targeted fictitious phishing emails using real-world scenarios to train staff to spot phishing attempts.
In summary, by implementing the cyber activities detailed in the two EDs and one Binding Operational Directive(BOD) while leveraging the Agency's advanced cybersecurity tools and technologies that detect and mitigate malware attacks, phishing emails, and unauthorized data exfiltration, USAID has reduced its cybersecurity risks to its network and data and protected its workforce while continuing to deliver on its mission in more than 80 countries around the world.

Independent Assessment

United States Agency for International Development (USAID's) information security program was evaluated as part of the FY 2022 FISMA Evaluation, which was conducted by an independent auditor. This evaluation included a review of a sample of 6 of 60 USAID internal and external information systems in USAID's FISMA inventory as of February 11, 2022. CLA's FY 2022 FISMA Evaluation noted that USAID implemented an effective information security program and practices by achieving an overall Optimized maturity level for the 20 core metrics based on the FY 2022 IG FISMA Reporting Metrics.

FY2022 Annual Cybersecurity Performance Summary

Department of Agriculture

Framework	CIO Rating	IGRating
Identify	15	Managed and Measurable
Protect	30.8	Defined
Detect	5	Consistently Implemented
Respond	15	Managed and Measurable
Recover	14.3	Consistently Implemented
Overall	80%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	8	6
E-mail	3	11	21
External/Removable Media	0	6	0
Impersonation	1	0	0
Improper Usage	132	74	181
Loss or Theft of Equipment	7	25	162
Web	14	14	91
Other	149	507	831
Multiple Attack Vectors	1	1	0
Total	308	646	1292

CIO Self-Assessment

Several enterprise-wide security capabilities were initiated or enhanced in FY2022 to address cybersecurity risks. The enterprise log maturity level and the vulnerability disclosure program were enhanced and achieved their OMB targets. All externally facing systems were made available to vulnerability researchers. Strong multifactor authentication improvements were made to reduce the use of passwords for authentication. A project to automate detection and block unauthorized access to sensitive information was successful and will be expanded. USDA completed a training needs assessment using the NICE Framework and identified work-role certifications to inform development and provide new opportunities for its workforce. USDA partnered with CISA to assess its SOC capabilities to qualify and quantify gaps in coverage and inform and prioritize solutions.

USDA implemented 22 GAO and IG audit findings in FY2022. As a result of maturing the information security program, the maturity of two Cybersecurity Framework functions (Identity and Recover) tested in the IG FISMA assessment improved from Consistently Implemented to Managed and Measurable. USDA continues to employ guidance and improve processes to achieve compliance while securing USDA networks and systems.

Independent Assessment

During FY 2022, we evaluated the effectiveness of the Department’s overall IT security program by evaluating FY 2022 Core IG Metrics at the entity level and for a subset of USDA's information systems. More specifically, we inspected a list of USDA Reportable Information Systems. Based on the analysis performed by an independent auditor and the OIG, we selected three centers from the USDA Office of the Chief Information Officer (OCIO), which were the CEC, the DISC, and the ISC. Of the 62 systems from the three selected centers, we took a representative sample of USDA information systems and conducted system level testing for 8 of the selected USDA information systems (3 contractor systems and 5 government systems). We also evaluated the implementation of prior year recommendations related to the Core IG Metrics. Consistent with applicable FISMA requirements, OMB policy and guidelines, and NIST standards and guidelines, USDA management has established and maintained its information security program and practices for the 5 Cybersecurity Functions and 9 FISMA Metric Domains. We assessed USDA's information security program and practices as Consistently Implemented (Level 3) based on a simple majority of the component scores for each Cybersecurity Domain’s maturity level. According to CyberScope and OMB's guidance, Managed and Measurable (Level 4) was effective; therefore, USDAs information security program is ineffective. As of 7/30/2022, we identified 4 findings: 1 for RM, 1 for IAM, 1 for ISCM, and 1 for IR. To improve its information security program, we recommend that the Department remediates vulnerabilities within its defined period. Furthermore, we recommend that the Department implements NIST SP 800-53, Rev 5, and ongoing authorization to improve its information security posture and continuous monitoring program. We recommend that the Department ensures mission area personnel are properly trained in identifying and reporting PII incidents and breaches.

FY2022 Annual Cybersecurity Performance Summary

Department of Commerce

Framework	CIO Rating	IGRating
Identify	15	Consistently Implemented
Protect	30.8	Defined
Detect	3.8	Defined
Respond	15	Consistently Implemented
Recover	11.3	Defined
Overall	76%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	3	0	10
E-mail	402	423	151
External/Removable Media	0	0	0
Impersonation	6	0	0
Improper Usage	851	417	378
Loss or Theft of Equipment	38	32	37
Web	114	42	59
Other	276	274	234
Multiple Attack Vectors	33	5	0
Total	1,723	1,193	869

CIO Self-Assessment

The Department of Commerce (DOC) continues its commitment to building a strong cybersecurity program that protects and enables its diverse mission. Between FY2021-FY2022, the DOC implemented a structured and systematic approach to increase cybersecurity visibility; consolidate cybersecurity structures and workflows; address gaps in people, process, and technology while identifying and reducing enterprise-wide Cybersecurity risks. The Department's Cybersecurity Program seeks to enable desired mission outcomes through exceptional leadership and execution by providing Department-wide:

*Security architecture, technology direction, and support resulting in mature, modern, and cost-effective solutions. The Department transition to a ZTA will be guided by the Department's ZTA Strategy and fulfills the objectives outlined by Executive Order 14028 on Improving the Nation's Cybersecurity to transform how we approach cybersecurity.

*Cyber defense operations, coordination, and support to reduce the likelihood and impact of cybersecurity attacks. By continuing to strengthen the Department cyber threat intelligence (CTI) sharing, and the deploying of an enterprise EDR capability, as well as proactive threat hunting and detection efforts employing forward-leaning capabilities (e.g., Artificial Intelligence (AI), Machine Learning (ML)), the Department will ensure that its cybersecurity personnel have the resources to carry out essential activities and limit potential harm to the Department

*Security program management, coordination, and governance, to ensure substantial risk reduction and increased compliance with Federal legislative and policy requirements.

*Dedicated commitment to promote and coordinate a highly skilled and diverse cybersecurity community working collaboratively to advance our shared vision.

Independent Assessment

The Department of Commerce (Department), Office of the Inspector General (OIG) completed an audit of the Department's information security program. OIG reviewed a representative subset of 10 information technology (IT) systems across the Department and its bureaus. OIG assessed 20 core FISMA metrics across five function areas and found the Identify and Respond function areas achieved a maturity level of 3, while the Protect, Detect, and Recover function areas achieved a maturity level of 2. While the Department defined policies and procedures, it did not consistently implement those policies and procedures across the selected systems. As a result, the Department's information security program has scored an overall maturity rating of level 2 (Defined) and is therefore not fully effective.

FY2022 Annual Cybersecurity Performance Summary

Department of Education

Framework	CIO Rating	IGRating
Identify	15	Consistently Implemented
Protect	34.9	Managed and Measurable
Detect	6.7	Managed and Measurable
Respond	15	Managed and Measurable
Recover	15	Managed and Measurable
Overall	87%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	1	0
E-mail	1	1	3
External/Removable Media	0	0	0
Impersonation	1	0	0
Improper Usage	51	44	9
Loss or Theft of Equipment	0	1	0
Web	5	1	6
Other	0	45	100
Multiple Attack Vectors	0	1	0
Total	59	94	118

CIO Self-Assessment

Throughout this year, the Department implemented tools, processes, and protections to maximize the quality, security, and privacy of our information systems. It also continued to develop and implement uniform and consistent governance policies and standards to strengthen the Department's cybersecurity by enhancing the confidentiality, integrity, and availability of its information technology infrastructure, systems, and data. As a result, the Department received an overall FISMA assessment of "Effective," or a Level 4 Cybersecurity Maturity Level for FY2022, the highest score ever achieved by the Department since the scoring metrics were established in 2014. This score also marks a significant improvement from FY21, with seven of nine FISMA domains increasing in maturity levels.

Independent Assessment

Our objective was to assess the U.S. Department of Education's (Department) progress at improving the maturity of its security program and practices as required by the Federal Information Security Modernization Act of 2014. In the fiscal year 2022, our inspection focused on 20 core metrics within the 5 security functions and the 9 associated metric domains for cybersecurity management. To answer the objective, we evaluated the Department's security program using the 20 core Inspector General Reporting Metrics that were published for the fiscal year 2022 and issued by the Office of Management and Budget. We determined the Department's programs were consent with Level 3 - Consistently Implemented, which is considered not effective for four domains Risk Management, Supply Chain Risk Management, Identity and Access Management, and Data Protection and Privacy. Level 4- Managed and Measurable which is considered effective for five domains Configuration Management, Security Training, Information System Continuous Monitoring, Incident Response, and Contingency Planning.

FY2022 Annual Cybersecurity Performance Summary

Department of Energy

Framework	CIO Rating	IGRating
Identify	14.9	Consistently Implemented
Protect	21.5	Consistently Implemented
Detect	6.2	Consistently Implemented
Respond	15	Consistently Implemented
Recover	14.6	Managed and Measurable
Overall	72%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	5	9	9
E-mail	103	110	176
External/Removable Media	1	3	0
Impersonation	0	8	0
Improper Usage	270	273	340
Loss or Theft of Equipment	119	179	139
Web	10	48	15
Other	215	70	230
Multiple Attack Vectors	4	0	0
Total	727	700	909

CIO Self-Assessment

Cybersecurity remains a top priority of the DOE, where its diverse mission underscores the need for leadership across the agency to play an active role in shaping cybersecurity risk management and mitigation activities. DOE faces cybersecurity threats such as phishing, malware, and advanced persistent threats, which are enhanced by the hybrid working environment and the increased sophistication of cyber threat actors and methods. Lack of funding and resources to modernize and secure IT and OT assets increases the risk of threat actors exploiting existing vulnerabilities. DOE is committed to reducing the risk of unauthorized access, damage, or disruption to business and mission critical systems. In FY 2022, DOE took a risk-based approach on its efforts to support cloud adoption, implement multifactor authentication and encryption, strengthen workforce/role-based training, and migrate to zero trust architecture. DOE will continue to focus on strengthening enterprise situational awareness; combating advanced persistent threats; forging interagency and sector partnerships to protect critical infrastructure; promoting information sharing; protecting sensitive information; enhancing policy and guidance; and advancing technologies for cyber defense to safeguard the agency's mission-critical assets.

Independent Assessment

The Office of Inspector General (OIG) conducted the annual evaluation of the Department of Energy's unclassified information security program and obtained results from the Department's Office of Enterprise Assessments related to its assessment of national security systems. Specifically, the OIG and Office of Enterprise Assessments reviewed the Department's progress towards meeting the DHS/OMB FY 2022 core FISMA cybersecurity metrics for the unclassified and national security cybersecurity programs systems at nine judgmentally selected sites. The cybersecurity programs were reviewed to assess the effectiveness of information security policies, procedures, and practices. Overall, the OIG determined that the Department was generally not effective in implementing the FY 2022 core FISMA cybersecurity metrics at the sites reviewed. While the OIG determined that the Department had achieved a Managed and Measurable (Level 4) maturity level for the Recover function, the remaining function areas (Identify, Protect, Detect, and Respond) were assessed at Consistently Implemented (Level 3), and the OIG noted that improvements should continue to be made in those areas. However, due to the nonhomogeneous nature of the Department's population, the OIG noted that it is likely that the weaknesses discovered at certain sites reviewed may not be representative of the Department's enterprise, 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.

FY2022 Annual Cybersecurity Performance Summary

Department of Homeland Security

Framework	CIO Rating	IGRating
Identify	14.6	Managed and Measurable
Protect	37	Managed and Measurable
Detect	5.7	Consistently Implemented
Respond	15	Managed and Measurable
Recover	13.4	Managed and Measurable
Overall	86%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	2	0
E-mail	311	25	19
External/Removable Media	17	1	0
Impersonation	0	0	0
Improper Usage	121	522	803
Loss or Theft of Equipment	10	0	0
Web	41	11	16
Other	204	1,241	678
Multiple Attack Vectors	0	5	0
Total	705	1,807	1516

CIO Self-Assessment

DHS leads the Federal government in cybersecurity practices meeting the Administration’s priorities. In FY2022, DHS has made significant improvements in all ten of the Security Domains of the Executive Order 14028, “Improving the Nation’s Cybersecurity”. DHS actively monitors the Multifactor Authentication (MFA), Encryption-at-Rest, Encryption-in-Transit and Authority to Operate (ATO) status of all FISMA systems. The DHS CIO’s continuous focus on resolving expired ATOs and closing high risk Plans of Action & Milestones (POA&M). In addition, significant reductions have been made in system cybersecurity risks by standardizing toolsets for the management of assets. Authorization management has been improved by working intensively to support Component success in the use of the Department’s Cyber Security and Assessment (CSAM) governance portal. Risks and issues are highlighted in monthly cybersecurity reports where every Component is directed to mitigate risks and resolve vulnerabilities. The DHS CISO continues to mature Department cybersecurity oversight through the DHS CISO Council ensuring that challenges are addressed at an enterprise level through all component stakeholders. Recent events have made it clear that despite maintaining strong FISMA compliance, adversaries are willing and able to carry out sophisticated, well planned, and targeted attacks to achieve their goals. As a result, DHS has accelerated its Cyber Supply Chain Risk Management implementation efforts and continues to refine its Unified Cybersecurity Maturity Model (UCMM) to appropriately identify and address cybersecurity gaps. DHS continues migration to a Zero Trust Architecture while conducting risk-based and outcome driven FISMA systems and services certifications. DHS is currently hiring cybersecurity staff using the new Cyber Talent Management System to address DHS's ongoing challenges in recruiting and retaining individuals with the skills necessary to execute DHS's cybersecurity mission.

Independent Assessment

For FY 2022, DHS’ information security program was effective because the Department earned a maturity rating of “Managed and Measurable (Level 4)” in four of five functions. DHS can further improve the effectiveness of its information security program with stronger Department-wide execution of its policies, procedures, and practices at all components. For example, we identified: (1) systems are being operated without authority to operate; (2) POA&Ms created for known information security weaknesses not being mitigated timely; (3) security configuration settings are not being implemented for all systems tested; (4) identity and access weaknesses at selected components; (5) one component was running an unsupported version of a Windows operating system on a workstation; and (6) some components did not apply security patches timely to mitigate critical and high-risk security vulnerabilities on selected systems tested.

FY2022 Annual Cybersecurity Performance Summary

Department of Health and Human Services

Framework	CIO Rating	IGRating
Identify	14.8	Consistently Implemented
Protect	33.5	Consistently Implemented
Detect	9.8	Defined
Respond	15	Consistently Implemented
Recover	15	Defined
Overall	88%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	23	106	97
E-mail	798	1,507	1467
External/Removable Media	0	88	74
Impersonation	0	42	76
Improper Usage	3,493	3,188	4178
Loss or Theft of Equipment	326	475	734
Web	91	2,232	1780
Other	2,501	797	1746
Multiple Attack Vectors	11	0	0
Total	7,243	8,435	10152

CIO Self-Assessment

The cybersecurity threat landscape at HHS, the federal government, and the Healthcare and Public Health (HPH) Sector continues to evolve and grow increasingly complex. HHS' cybersecurity program has evolved and remains able to best protect the Department from those threats and assist the HPH sector in mitigating the risks from those threats. HHS continues to mature its Cybersecurity and Enterprise Risk Management (ERM) integration with a Cyber-ERM group for thought leadership and information sharing across HHS and its Operating Divisions. The High Value Asset (HVA) Program implemented additional security measures to ensure HVAs are prioritized based on risk impact and mission functionality. In FY22, HHS sent 881,144 phishing emails and conducted 114 ethical phishing scenarios; reviewed 91,341 URLs and reported 6,219 malicious websites for takedown; analyzed 44,836 reported spam messages, 1,519 of which were malicious and 90 of which triggered malicious site takedown requests; and researched 96 coordinated malspam campaigns. HHS continues to collaborate internally and with its federal partners including the Federal Bureau of Investigation (FBI) and CISA to develop options for enhanced cyber hygiene, threat detection, and information sharing; HHS also released over 80 new products to share actionable cybersecurity information, and over 36 new cybersecurity awareness products to improve resiliency and drive behavior change within the HPH sector. Additionally, HHS continues to respond to Executive Order 14028, Improving the Nation's Cybersecurity requirements including reports on multifactor authentication, data encryption; zero trust and cloud technology strategies; HVAs and data sensitivity; and EO-critical software.

Independent Assessment

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

FY2022 Annual Cybersecurity Performance Summary

Department of Housing and Urban Development

Framework	CIO Rating	IGRating
Identify	13.9	Consistently Implemented
Protect	31.2	Defined
Detect	5.9	Defined
Respond	15	Consistently Implemented
Recover	13.5	Consistently Implemented
Overall	80%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	0	1
E-mail	3	8	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	20	12	4
Loss or Theft of Equipment	0	0	0
Web	0	0	3
Other	15	10	3
Multiple Attack Vectors	0	0	0
Total	38	30	11

CIO Self-Assessment

This summary highlights the steps that the Department of Housing and Urban Development (HUD) has undertaken in Fiscal Year (FY) 2022 to mitigate and prevent cybersecurity risks to create a cyber safe Agency. In FY 2022, HUD has continued to take significant measures to inform HUD employees of the dangers of cyber vulnerabilities and risks of remote work through the increase in monitoring for cybersecurity awareness, conducting targeted personnel trainings, and facilitating phishing campaigns to provide additional awareness to users who clicked during phishing exercises. Specifically, the measures were performed through FY 2022 Phishing Exercises and the Ransomware IR/Contingency Planning tabletop exercise for OCIO. In the past 12 months, HUD has initiated a Data Loss Prevention (DLP) Program and enabled a data classification and discovery capability that prevents external sharing of data that contain sensitive data including personally identifiable information (PII) and financial data. Overall, HUD has closed 45 OCIO and Privacy aligned audit recommendations, operationalized three Cyber Dashboard domain views, and developed/updated several policies, procedures, and templates that address the spectrum of HUD's risk management process. In the upcoming Fiscal year, HUD is looking to improve upon its current cybersecurity posture through the expansion of trained and cyber-aware staff, enhancements of data protection capabilities, continued enrollment of systems into the information security continuous monitoring (ISCM) program, transition to NIST 800-53 Revision 5, and maturation of cybersecurity related capabilities.

Independent Assessment

HUD continued to take positive steps to improve its information technology (IT) security posture, increasing maturity in 3 of the 20 core metrics assessed in FY 2022. However, it maintained an overall ineffective IS program and dropped from the consistently implemented to defined maturity level based on the IG evaluation of 20 core metrics. HUD remained at the same maturity level for 16 of the 20 core metrics and dropped in maturity for 1 core metric. These changes in maturity were consistent with HUD's progress in previous fiscal years. HUD's overall drop in maturity could be attributed to the reduced number of scored metrics the IG was instructed to assess. HUD had previously reached the consistently implemented maturity level in both FY 2020 and FY 2021 when all IG metrics were required to be assessed. However, significant limitations and challenges continue to impact the Chief Information Officer's ability to establish an effective IS program. For FY 2022, budget and resource constraints negatively impacted HUD's ability to mature. This contributed to HUD's inability to develop, modernize, and enhance its IT environment, leaving large numbers of legacy systems. These systems continued to elevate risks to HUD's IT environment, were resource-intensive, and limited the effectiveness of the Office of the Chief Information Officer to acquire and deploy technology necessary to implement critical security controls. Finally, HUD continued to face challenges with efficiently awarding IT contracts and conducting contractor oversight.

FY2022 Annual Cybersecurity Performance Summary

Department of the Interior

Framework	CIO Rating	IGRating
Identify	14.5	Consistently Implemented
Protect	20.6	Managed and Measurable
Detect	2.8	Managed and Measurable
Respond	15	Consistently Implemented
Recover	15	Consistently Implemented
Overall	68%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	0	2
E-mail	10	33	59
External/Removable Media	0	0	2
Impersonation	0	1	1
Improper Usage	164	35	72
Loss or Theft of Equipment	0	6	12
Web	19	75	61
Other	169	117	60
Multiple Attack Vectors	0	10	0
Total	363	277	269

CIO Self-Assessment

DOI responded to the issuance of Executive Order 14028 and subsequent OMB memoranda by committing to bold, transformative actions to prioritize, modernize, and secure IT resources and assets and to build toward modernization that is essential to developing a Zero Trust architecture (ZTA). DOI has developed a three-pronged approach to achieving its ZTA goals: (1) Modernize enterprise networks by employing software-defined technologies to holistically secure endpoints, decommission legacy perimeter infrastructure, and continuously verify devices after authentication. (2) Provide a comprehensive understanding of DOI's data assets and the sensitivity, value, and threats to those assets. (3) Build a robust enterprise identity management system, underpinned by adoption of impersonation-resistant multifactor authentication (MFA) solutions, that can be integrated into applications and common platforms. Currently DOI requires PIV authentication for its domain administration accounts and all enterprise directory accounts with elevated privileges, as well as for all VPN access. In August 2022, DOI directed its components to enforce MFA for all information systems through approved phishing-resistant MFA services by the end of 2024. For instances where passwords are required, DOI is revising its password policies to increase minimum password length and remove dated complexity requirements that lead users to create weaker passwords. In FY 2022, the Department closed 57 information technology (IT) audit recommendations. DOI had no major security incidents or privacy breaches that required reporting to Congress and detected no incidents that resulted in significant compromise. DOI continues to implement enhancements to Endpoint Detection and Response (EDR) capabilities to mitigate the risk of commercial product exploits.

Independent Assessment

We conducted a Performance Audit over the Department of the Interior's (DOI) information security program and practices for the FY 2022. The scope of the performance audit included following 11 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 Solicitor (SOL), and U.S. Geological Survey (USGS). DOI had 197 operational unclassified information systems, and we randomly selected 16 information systems across the 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, according to OMB criteria, the program was not effective as weaknesses were identified three of five function areas, Identify, Respond, and Recover. The Protect and Detect function areas were effective. Weaknesses were noted in the FISMA domain areas of risk management, supply chain risk management, configuration management, security training, incident response, and contingency planning domains. The identity and access management, data protection and privacy, and information security continuous monitoring domains were effective.

We assessed the cybersecurity Protect and Detect functions at Managed and Measurable (Level 4) and Identify, Respond and Recover functions at Consistently Implemented (Level 3). Overall, we assessed DOI's information security program and practices for as Consistently Implemented (Level 3) based on a simple majority of the component scores for each Cybersecurity Domain's maturity level

FY2022 Annual Cybersecurity Performance Summary

Department of Justice

Framework	CIO Rating	IGRating
Identify	15	Managed and Measurable
Protect	37	Managed and Measurable
Detect	6	Consistently Implemented
Respond	15	Optimized
Recover	15	Consistently Implemented
Overall	88%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	2	0	8
E-mail	246	200	93
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	114	90	20
Loss or Theft of Equipment	3	3	1
Web	2	1	2
Other	81	113	80
Multiple Attack Vectors	2	0	0
Total	450	407	204

CIO Self-Assessment

The Office of the Chief Information Officer has continued to advance the Department's cybersecurity program, including automation of endpoint detection and response and data exfiltration prevention. Integrating continuous monitoring outputs within the Department's robust GRC platform, CSAM A&A, provides stakeholders near real-time access to vulnerability, configuration, and asset inventory management information, empowering decisionmakers with system risk insight for timely response actions. The Department's attainment of an "Optimized" rating from the Office of the Inspector General for the Respond function and "Managed and Measurable" for both Identify and Protect is attributable to the Department's systematic program maturation. While the OIG's assessment reflects overall elevation of the Department's cybersecurity function areas, it also identified opportunities for improvement. In response to these assessments, and through the Department's recent budget submission to OMB, the Department will continue to drive enterprise-wide adoption of strong access controls with multifactor authentication, including using Homeland Security Presidential Directive-12 Personal Identity Verification and other phishing-resistant solutions for external users and situations. The Department will also continue to seek efficient and cost-effective solutions to data-storage challenges associated with enhanced logging and log retention capabilities. In addition, the Department will focus on systematically conducting business impact analyses and contingency planning, and rigorous patch management that balances operational need with cybersecurity protection. By addressing these challenges, the Department expects to elevate its Recover and Detect functions from their current "Consistently Implemented" rating.

Independent Assessment

During fiscal year 2022, the Department of Justice (Department) Office of the Inspector General (OIG) reviewed the information security programs of 6 Department components and a sample of 14 systems within these components. As a result of our review, the OIG determined that the maturity level for the Department's information security program is "Level 3 – Consistently Implemented" for two security functions, Detect and Recover; "Level 4 – Managed and Measurable" for two security functions, Identify and Protect; and "Level 5 – Optimized" for one security function, Respond. Based on the OIG's review, we determined that the Identify, Protect, and Respond security functions are effective; the Detect and Recover security functions are not effective; and the overall information security program for the Department is effective. It should be noted that the OIG's assessment this fiscal year included a select group of 20 core metrics that must be evaluated annually, and the remaining metrics will be evaluated on a 2-year cycle. Therefore, the Department should implement our recommendations specifically within the Risk Management, Configuration Management, Identity and Access Management, Data Protection and Privacy, Information Security Continuous Monitoring, and Contingency Planning metrics of the Identify, Protect, Detect, and Recover Functions to improve the effectiveness of the Department's information security program.

FY2022 Annual Cybersecurity Performance Summary

Department of Labor

Framework	CIO Rating	IGRating
Identify	15	Consistently Implemented
Protect	34.9	Consistently Implemented
Detect	5.1	Defined
Respond	15	Managed and Measurable
Recover	15	Consistently Implemented
Overall	85%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	7	3
E-mail	17	30	64
External/Removable Media	0	0	0
Impersonation	0	0	14
Improper Usage	111	190	224
Loss or Theft of Equipment	80	59	132
Web	5	4	135
Other	109	105	4
Multiple Attack Vectors	2	1	0
Total	325	396	576

CIO Self-Assessment

In FY 2022, DOL continued to enhance the cybersecurity program, including for areas prioritized under EO 14028. The Department continues to implement enterprise-wide solutions to enhance encryption, multifactor authentication, information technology asset management, incident response, and monitoring. DOL made progress toward the deployment of DHS CDM tools for vulnerability management, continued implementation of new Data Loss Prevention mechanisms, and fully transitioned all FISMA systems into Ongoing Authorization. In the areas of privacy, DOL updated a privacy teleworking guide to help DOL staff and contractors secure personally identifiable information while working remotely. As a part of DOL's Cybersecurity and Privacy Awareness, DOL successfully carried out its annual Cybersecurity Awareness Month and other awareness initiatives to reinforce cybersecurity and privacy policies and guidance. Additionally, DOL conducted quarterly phishing exercises to promote phishing awareness.

In the area of incident detection and response, DOL continues to collaborate with DHS to take a more automated approach to incident response, and successfully expanded the Vulnerability Disclosure Program.

Looking ahead, DOL will continue to focus on strengthening its cybersecurity management functions, particularly for areas prioritized under EO 14028. DOL intends to continue to improve in the adoption of MFA and encryption of data-at-rest and in-transit; continue the monitoring and protection of critical software and mature capabilities for supply chain risk management; continue efforts to transition DOL's network infrastructure to IPv6; improve DOL's enterprise log management capability in accordance with OMB M-21-31; continue the implementation of DOL's roadmap for Zero Trust; and, continue Security Operations Center enhancements that will allow the Department to anticipate and mitigate risk, and stay ahead of the evolving threat landscape.

Independent Assessment

DOL-OIG contracted with KPMG to conduct the FY 2022 evaluation of DOL's information security program required by FISMA. Our scope included assessing the maturity levels for the FY 2022 IG FISMA Reporting Metrics and testing the NIST 800-53 security controls referenced in these metrics at the entity level, for 16 of 54 selected DOL operated information systems, and for 4 of 17 selected contractor information systems. In addition, we followed up on the status of 20 of DOL's prior-year FISMA recommendations and determined 5 were closed.

We assessed the overall DOL IT security program as not effective based on the mode of the individually assessed maturity levels for the FY 22 Core IG Metrics. Specifically, we identified 10 issues that were consolidated into 8 findings for the FY 2022 performance audit report. The nature of these findings affected our overall assessment of the Cybersecurity Functions.

To improve its information security program, DOL should update and implement its security policies and procedures to be compliant with NIST 800-53, Revision 5. DOL should design, implement, and monitor qualitative and quantitative key performance indicators to measure the effectiveness of its Identify and Recover processes and enhance its key performance indicators for Configuration Management and Identity and Access Management. Additionally, DOL should develop and implement Plans of Action and Milestones (POA&Ms) to remediate the 8 FY 2022 audit findings and all open prior-year IT security program recommendations.

FY2022 Annual Cybersecurity Performance Summary

Department of State

Framework	CIO Rating	IGRating
Identify	11.3	Defined
Protect	27.5	Consistently Implemented
Detect	5	Defined
Respond	15	Managed and Measurable
Recover	15	Defined
Overall	74%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	6	2	0
E-mail	289	18	47
External/Removable Media	1	2	7
Impersonation	3	0	0
Improper Usage	631	559	381
Loss or Theft of Equipment	3	7	17
Web	110	13	53
Other	192	181	192
Multiple Attack Vectors	16	6	0
Total	1,251	788	697

CIO Self-Assessment

The Department of State FY2022 Annual FISMA Report continues to demonstrate its efforts to improve IT security by prioritizing and aligning its efforts to Executive Order (EO) 14028. The Zero Trust (ZT) implementation will enable the Department to effectively identify, protect from, detect, respond to, and recover from critical threats in the cyberspace. The Department has developed a Zero Trust Strategy/ Integrated Governance Plan to oversee the ongoing improvements as well as an Identity, Credential, and Access Management (ICAM) Working Group to assist stakeholders and assign areas of responsibility. In addition, the Department has already established the NIST Supply Chain Risk Management Framework to identify Critical Software and secure IT hardware and software purchases. With regard to Audit Logging, the Department is exploring the possibility of data lake strategy to meet the significant storage requirements for M-21-31 log retention and wants to use existing as well as new technology to meet this requirement. The Department continues to concentrate on improving the percentages of both High and Moderate Impact Systems that have been authorized. Currently the percentage of High Impact Systems authorized is 92 % while the percentage of Moderate Impact Systems authorized has reached 86 %. The Department has authorized 93 % of their High Value Asset (HVA) Systems. The Department has also shown improvements in encrypting Data-in-Transit at 86 % of systems, encrypting Data-at-Rest at 76 % of systems, and Multi-Factor Authentication at 70 % of systems comprising the Department's Inventory.

Independent Assessment

The Department of State (Department) Office of Inspector General (OIG) and OIG’s independent contractor assessed the information security program of the Department as not effective for FY 2022. The assessment scope included a selection of the Department’s major, Federal Information Security Modernization Act of 2014 (FISMA)-reportable information systems. OIG’s independent contractor found that the Department had taken steps to establish an organization-wide information security program by generally developing and implementing certain activities that support the Department’s operations and assets. However, the assessment identified areas throughout eight of the nine domains where planned improvements or development of new activities and controls were not finalized and operating during the scope period. As such, based on the FY 2022 IG FISMA Reporting Metrics, the Department operated its information security program at an overall level 2, defined, maturity. OIG intends to issue a FISMA audit report by the end of FY 2022 and has preliminarily communicated to Department management that the assessment resulted in 8 new recommendations, as well as a determination that 17 of 21 recommendations from previous FISMA audits that directly related to the FY 2022 IG FISMA Reporting Metrics remained open as of the FY 2022 FISMA Audit Report.

FY2022 Annual Cybersecurity Performance Summary

Department of Transportation

Framework	CIO Rating	IGRating
Identify	14.9	Defined
Protect	25.3	Defined
Detect	2.5	Defined
Respond	15	Consistently Implemented
Recover	15	Consistently Implemented
Overall	73%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	3	2	5
E-mail	6	13	24
External/Removable Media	3	0	14
Impersonation	1	1	1
Improper Usage	85	67	292
Loss or Theft of Equipment	1	3	3
Web	25	26	18
Other	130	248	241
Multiple Attack Vectors	5	2	0
Total	259	362	598

CIO Self-Assessment

The OCIO recognizes that the successful execution of the Department's cybersecurity program is grounded in partnership across the Department, its OAs, external stakeholders, and the OIG. The DOT has an extensive cybersecurity management program, with multiple lines of effort and coverage across the agency's enterprise. With the leadership and support of a new agency CIO, DOT maintained momentum on multiple fronts in support of Executive Order (EO) 14028, direction from the OMB, and enhanced attention on key initiatives through prioritization of dedicated resources. The CIO immediately set the tone at the start of his term by identifying cybersecurity as the Department's top IT priority. A new Departmental CISO was hired on Aug 2022. Over the last year and a half, DOT accomplished the following: reduced the number of exceptions from mandatory use of Personal Identity Verification (PIV) cards for unprivileged, multi-factor authentication to agency networks from 1,919 to 315 users; conducted an agency-wide contingency exercise led by the Secretary and DOT senior appointee and career leadership; reviewed agency critical functions and systems, potential mission impacts, and lessons-learned to inform future planning, and investment; updated the MOU between the DOT CIO and the FAA for the enterprise SOC, clarifying agency roles and responsibilities and establishing a framework for developing future enterprise incident response capabilities and achieving initial operational capability for the agency Continuous Diagnostics and Mitigation (CDM) dashboard. The CIO charged the new CISO to expedite the hiring of highly qualified cybersecurity professionals needed to support a Department with a broad mandate and diverse missions, such as DOT. The CIO and the CISO have continued to focus on securing the enterprise and addressing the OIG's findings to ensure that the Department consistently enforces an agency-wide cybersecurity program.

Independent Assessment

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

FY2022 Annual Cybersecurity Performance Summary

Department of the Treasury

Framework	CIO Rating	IGRating
Identify	15	Consistently Implemented
Protect	29.7	Managed and Measurable
Detect	6.1	Consistently Implemented
Respond	15	Managed and Measurable
Recover	15	Consistently Implemented
Overall	81%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	4	2	3
E-mail	7	2	3
External/Removable Media	1	0	0
Impersonation	0	0	0
Improper Usage	139	154	98
Loss or Theft of Equipment	5	3	3
Web	1	2	0
Other	49	80	19
Multiple Attack Vectors	0	1	0
Total	206	244	126

CIO Self-Assessment

The mission of the Department of the Treasury is to maintain a strong economy and promote conditions that enable economic growth and stability at home and abroad, strengthen national security by combating threats and protecting the integrity of the financial system, and effectively manage the United States government’s finances and resources. To execute this mission, Treasury must store, process, transmit, and share large volumes of sensitive financial and personal information pertaining to the transaction of trillions of dollars. Treasury faces inherent cybersecurity risks in the interactions with both private and other public sector organizations, limitations of authentication technologies, reliance on externally managed critical infrastructure, and a current lack of centralized visibility of agency information technology assets and networks. The likelihood of risk realization is magnified by the expansion of telework and continuing evolution in the volume, sophistication, and frequency of cyber threats. Treasury leadership remains engaged in the development of plans to address these risks. Throughout FY2022, Treasury continued to leverage investments from supplemental funding provided through the Cybersecurity Enhancement Account to mitigate cybersecurity risks. To proactively address increased risks, Treasury continued to develop the Enterprise Cyber Risk Management with an enhancement of the Supply Chain Risk Management program. These programs address vulnerabilities that affect Treasury assets that could be exploited. An SCRM Strategy and Enterprise Vulnerability Management Plan were created to address supply chain protection and responses to BOD 22-01. FY 2022 CIO FISMA metrics were overhauled from past years’ Cross-Agency Priority requirements. The FY 2022 FISMA included ten new sections focusing on the federal government’s ability to conduct tested security. Treasury has made significant progress towards achieving the requirements of EO 14028.

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 NSSs for the 5 Cybersecurity Functions and 9 FISMA Metric Domains.

However, the program was ineffective, according to OMB criteria, as reflected by the 4 unclassified findings noted within 3 of the 5 Cybersecurity Functions, within 4 of the 9 FISMA Metric Domains and reflected by the 2 collateral findings noted within 1 of the 5 Cybersecurity Functions, within 2 of the 9 FISMA Metric Domains. We assessed Identity and Access Management, Data Protection and Privacy, and Incident Response, as Managed and Measurable (Level 4). Further, we assessed Risk Management, Supply Chain Risk Management, Security Training, Information Security Continuous Monitoring, and Contingency Planning as Consistently Implemented (Level 3). Finally, we assessed Configuration Management as Defined (Level 2).

Overall, we assessed the Treasury’s Information Security program and practices for unclassified systems at Level 4 (Managed and Measurable) and collateral NSSs as Consistently Implemented (Level 3). Collectively, Treasury was assessed a Level 3, which is ineffective according to OMB guidance.

FY2022 Annual Cybersecurity Performance Summary

Department of Veterans Affairs

Framework	CIO Rating	IGRating
Identify	15	Defined
Protect	33.3	Defined
Detect	7.5	Defined
Respond	15	Managed and Measurable
Recover	15	Defined
Overall	86%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	0	0
E-mail	233	166	135
External/Removable Media	0	4	3
Impersonation	0	3	3
Improper Usage	21	104	96
Loss or Theft of Equipment	302	593	900
Web	7	211	144
Other	375	0	0
Multiple Attack Vectors	3	0	0
Total	941	1,081	1281

CIO Self-Assessment

The Department worked aggressively to improve its information security controls in FY 2022 and considers implementation of our Zero Trust First Cybersecurity Strategy critical to enhancing and maintaining a strong cybersecurity posture. Of note, while VA continues working to address the FISMA audit recommendations and restructuring its programs to address the Material Weakness, the Executive Order (EO) 14028: Improving the Nations Cybersecurity was signed on May 12, 2021, and as a result, 55+ new requirements have been added to our Cybersecurity program. This has caused VA to assess the appropriate balance of priorities between these two regulatory structures. VA has significantly strengthened its risk management process in FY 2022 in the following areas:
•Deployed Endpoint Detection Response (EDR) to 579,505 total endpoints, of which 577,661 were on-prem and 1,844 in the cloud;
•Implemented comprehensive security vulnerability management with more than 93% of all vulnerabilities consistently managed, well above industry standard of approximately 70%;
•Enforced mandatory Personal Identity Verification (PIV) requirements for 9 additional Medical Systems and partially remediated PIV non-compliance for 3 additional Medical Systems bringing the total enterprise to 96%;
•Reduced or removed banned devices in use in accordance with Section 889 of the 2019 National Defense Authorization Act (NDAA) by 80%;
•Spearheaded the adoption of the Integration Control Number (ICN) as an alternative to Social Security (SSN) for SSN reduction and elimination;
•Developed a Modernization Strategy and Cybersecurity Strategy to speak directly to the current material weakness and the importance of a Zero Trust First security posture.
Improvements in continuous monitoring through aggressive implementation of the DHS's CDM Program, coupled with VA's enterprise-wide information security initiatives, continue to provide a path forward.

Independent Assessment

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

FY2022 Annual Cybersecurity Performance Summary

Environmental Protection Agency

Framework	CIO Rating	IGRating
Identify	14.9	Consistently Implemented
Protect	33.6	Consistently Implemented
Detect	5	Consistently Implemented
Respond	15	Consistently Implemented
Recover	15	Consistently Implemented
Overall	83%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	0	0
E-mail	11	15	9
External/Removable Media	0	1	0
Impersonation	0	0	0
Improper Usage	15	1	25
Loss or Theft of Equipment	37	40	49
Web	8	22	15
Other	36	16	1
Multiple Attack Vectors	3	0	0
Total	110	95	99

CIO Self-Assessment

In FY22 EPA has managed agency risk through vigilance, continued strengthening of our cyber defenses, and risk management processes. EPA continues efforts to manage risks associated with remote access management resulting from a hybrid workforce such as privileged network access management, the continued implementation of PIV enforced multi-factor authentication and alternative two factor authentication mechanisms for privileged and non-privileged users. To address risks associated with unauthorized access, data encryption, and data exfiltration; the EPA supported the National Security Council Cyber Sprint and seen increased adoption for encryption supporting Data at Rest and Data in Transit. EPA has also made notable progress in the continued efforts for Data Loss Prevention (DLP) capability for email, shared drive environments, other collaboration tools. In FY 2022, the agency deployed an Enterprise solution to prevent the usage of untrusted removable media provide added protections to safeguard its operational environments. The EPA has implemented an Enterprise Endpoint Detection and Response solution enabling near real-time identification, analysis, and remediation of Cybersecurity incidents and proactive prioritization of cyber threat response activities. In FY2023 and beyond, the EPA will continue focused efforts to achieve the overall objective of the federal cyber security requirements, including Executive Order 14028 and various supporting DHS directives and OMB memoranda to defend against cyber threats, risks, and safeguard our assets.

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 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 2022 Inspector General Federal Information Security Modernization Act, or FISMA, Reporting Metrics. While the EPA has policies, procedures, and strategies implemented for these function areas and a majority of the domains, improvements are still needed in the following areas:

• Risk Management – the EPA lacks documentation of an annual review of the system security plan and implemented or inherited controls around automated tools used in risk assessments for the sampled Analytical Radiation Data System.

• Configuration Management – For the sampled Analytical Radiation Data System, we found the Agency did not:

•Create plans of action and milestones to track the remediation of a sample of eight randomly selected critical vulnerabilities within two days as required by the Agency’s Chief Information Officer Directive 2150-P-17.2, Information Security – Interim System and Information Integrity Procedures.

•With respect to FY Core IG Metrics Question 21, apply patches to remediate vulnerabilities in a timely manner as required by Directive 2150-P-17.2.

FY2022 Annual Cybersecurity Performance Summary

General Services Administration

Framework	CIO Rating	IGRating
Identify	15	Optimized
Protect	36.2	Optimized
Detect	12.3	Optimized
Respond	15	Optimized
Recover	15	Managed and Measurable
Overall	94%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	1	1	0
E-mail	3	16	30
External/Removable Media	0	0	0
Impersonation	1	0	1
Improper Usage	68	19	15
Loss or Theft of Equipment	0	0	0
Web	7	25	35
Other	22	21	9
Multiple Attack Vectors	0	0	2
Total	102	82	92

CIO Self-Assessment

In FY2022, GSA aligned its cyber security strategy to the requirements within the President’s Executive Order (EO) for Improving the Nation’s Cybersecurity focused on Zero Trust. The agency focused on reducing risk and strengthening resilience while maintaining an effective and compliant program overall. GSA continued its movement towards enterprise shared services, a shift left security model that prioritizes continuous innovation, continuous improvement, and DevSecOps. Risks and related mitigations faced in FY2022 are below:

(1) Phishing: Continuous phishing campaign using anti-phishing tools and threat simulations; enhanced security awareness training; BOD 18-01 security; and Email URL analysis and Executable sandboxing.

(2) Malware and Cyber Hacking: Continued maturation of key technologies including but not limited to: Enterprise Network Deception; Automated Red and Blue Team; Vulnerability Disclosure Policy and Bug Bounty; SOC and IR; Enterprise Logging with machine learning; M-21-30 implementation; and, Cyber threat hunting.

(3) OT/IOT Security: Achieved micro segmentation for 90 GSA buildings to further secure Operational Technology/Internet of Things (OT/IOT) devices supporting building operations; and Hardware/Software device testing via Device Testing Lab.

(4) Remote Work Security: Deployed Secure Access Service Edge (SASE); and enhanced GSA Security Operations Center visibility and threat detection/response capabilities with advanced Machine Learning / Artificial Intelligence models focusing on lateral movement and user behavior analytics.

(5) Cyber Supply Chain Risk Management (C-SCRM): Enhanced our capabilities to identify devices that are counterfeit, compromised, or from a prohibited vendor; expanded our supplier illumination toolset for monitoring critical vendors; and initiated processes for incorporating C-SCRM into the pre-award acquisitions.

Independent Assessment

For the Independent Performance Audit on the Effectiveness of the U.S. General Services Administration’s (GSA) Information Security Program and Practices for FY 2022, our scope included assessing the maturity levels for the FY 2022 Core IG Metrics and testing the NIST Special Publication (SP) 800-53 security controls referenced in these metrics at the entity level, for 7 selected GSA-operated information systems, and for 3 selected contractor-operated information systems. In addition, we followed up on the status of 4 prior-year FISMA findings. Based on the work performed in FY 2022, we assessed the overall GSA IT security program as effective based on determining the mode of the individually assessed maturity levels for the 20 metrics, as directed by the OMB FY 2022 Core IG Metrics guidance. Specifically, we assessed the Identify, Protect, Detect, and Respond Cybersecurity Functions as Optimized (Level 5), while the Recover Cybersecurity Function was assessed as Managed and Measurable (Level 4). While GSA did close the 4 prior-year findings, we identified 1 new finding in the Risk Management (RM) FISMA Metric domain; 5 new findings in the Configuration Management (CM) FISMA Metric domain; and 6 new findings in the Identity and Access Management (IAM) FISMA Metric domain. The nature of these findings did not affect our overall assessment for any of the Identify and Protect Cybersecurity Functions. GSA should fully implement NIST SP 800-53, Revision 5, for its information security program. GSA should design and implement automated mechanisms for testing its contingency planning and improve controls related to Configuration Management and IAM. GSA should also develop and implement Plans of Action and Milestones (POA&Ms) to remediate FY 2022 audit findings.

FY2022 Annual Cybersecurity Performance Summary

National Aeronautics and Space Administration

Framework	CIO Rating	IGRating
Identify	15	Defined
Protect	28.3	Consistently Implemented
Detect	5.5	Defined
Respond	15	Consistently Implemented
Recover	15	Consistently Implemented
Overall	79%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	5	1	1
E-mail	11	46	28
External/Removable Media	2	34	37
Impersonation	0	4	1
Improper Usage	1,165	607	720
Loss or Theft of Equipment	3	288	1
Web	17	123	111
Other	417	91	734
Multiple Attack Vectors	6	0	0
Total	1,626	1,194	1633

CIO Self-Assessment

This year NASA transitioned from the largely remote workforce of COVID-19 to a more dynamic hybrid state where many workers and partners are onsite with NASA, while others remain predominantly remote and online. To facilitate the safe and secure access to NASA information technology in support of its science, exploration and aeronautics missions, NASA must guard against threats to our networks from unauthorized users, threats to our supply chain, and attacks on our internal networks, especially through web sites used by the public and NASA to share information. NASA mitigations to counter these threats have included establishing conditional access policies for secure information sharing to authorized users with non-NASA devices and launching a Proactive Supplier Engagement Process (PSEP) to introduce more efficiencies into NASA’s SCRM assessment activities and increase the speed of acquisitions of covered products. To better secure our web environments, NASA established a milestone date for preloading the nasa.gov domain and plans to ensure NASA web services meet all HTTPS compliance requirements to enable preloading without disruption.

Independent Assessment

NASA's information security program was evaluated as part of the FY2022 FISMA evaluation, which was conducted by RMA Associates (RMA). We assessed NASA's information security policies, procedures, and practices by examining four (4) of the Agency's information systems. We determined that information security continues to remain a challenge for NASA based on this evaluation and other reviews. While NASA continues to make progress in securing its networks and information systems, its cybersecurity program remains ineffective when assessed against OMB's model, which requires agencies to achieve a level 4 maturity (managed and measurable) to be considered effective. While NASA continues to make incremental improvements in its cybersecurity program, NASA information systems continue to remain vulnerable to internal and external cybersecurity threats.

FY2022 Annual Cybersecurity Performance Summary

National Science Foundation

Framework	CIO Rating	IGRating
Identify	15	Consistently Implemented
Protect	31.2	Consistently Implemented
Detect	5	Managed and Measurable
Respond	15	Managed and Measurable
Recover	15	Optimized
Overall	81%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	1	0
E-mail	1	1	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	1	0	1
Other	3	2	0
Multiple Attack Vectors	0	0	0
Total	5	5	1

CIO Self-Assessment

In FY 2022, NSF continued to adopt more advanced features and automated processes for managed detection and intelligence-led incident response services. NSF onboarded a new capability for its cloud services to enable advanced network detection. The managed detection and response service provides surge support and increases the NSF Security Operations Center's capability to provide rapid response and analysis of threats and priority events. NSF's use of automated threat detection tools has helped NSF significantly reduce its number of incidents by blocking network-based threats. NSF continues to grow the maturity of its security information and event management system (SIEM) by onboarding new data sources.

As suppliers and service providers are critical resources in the Foundation's cybersecurity program, NSF developed supply chain risk management guidance which outlines recommended security practices when acquiring IT products and services to mitigate potential risks in products, services, and solutions.

Independent Assessment

To assess whether the National Science Foundation (NSF) effectively implemented its agency-wide Information Security Program and practices for FY 2022, an independent auditor conducted a performance audit on behalf of NSF-OIG. The auditor performed detailed testing of NSF’s General Support System (GSS) and United States Antarctic Program (USAP) GSS for compliance with selected NIST standards and other controls as specified in the FY 2022 Inspector General FISMA Reporting Metrics.

Based on the audit, NSF’s Information Security Program was effective for FY 2022. The driving factor for this assessment was the consistent implementation and application of NSF’s control environment, which directly impacted NSF’s overall ratings. Improvements were achieved by developing and implementing corrective action plans in response to prior year deficiencies. However, some deficiencies remain unremedied. Specifically, NSF has been unable to fully implement corrective actions for long-standing weaknesses within the USAP GSS related to Identity and Access Management, Data Protection and Privacy, and Incident Response. NSF’s continued inability to remediate these weaknesses within the USAP GSS could impact NSF’s ability to achieve an overall rating of Effective in FY 2023.

To become more effective, NSF should ensure it implements plans of action and milestones (POA&Ms), especially those for the USAP GSS, in a timely manner to address findings identified during this audit and other self-assessments as well as comply with policy changes as they become due.

FY2022 Annual Cybersecurity Performance Summary

Nuclear Regulatory Commission

Framework	CIO Rating	IGRating
Identify	15	Managed and Measurable
Protect	38.4	Managed and Measurable
Detect	9	Managed and Measurable
Respond	15	Managed and Measurable
Recover	7.5	Consistently Implemented
Overall	85%	Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	0	0
E-mail	0	0	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	5	7	3
Loss or Theft of Equipment	0	1	0
Web	0	2	1
Other	4	1	1
Multiple Attack Vectors	1	0	0
Total	10	11	5

CIO Self-Assessment

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

Independent Assessment

An independent public accounting firm (IPA), under contract and supervision of the Nuclear Regulatory Commission (NRC) Office of the Inspector General (OIG), completed a performance audit to evaluate the effectiveness of NRC’s information security program and practices and to respond to the Office of Management and Budget (OMB) Fiscal Year (FY) 2022 Core Inspector General (IG) Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics.

The IPA’s methodology included testing the effectiveness of selected security controls implemented in a subset of systems in accordance with the NIST Special Publication (SP) 800-53, Revision (Rev.) 5, Security and Privacy Controls for Information Systems and Organizations.

In conclusion, the IPA determined that NRC implemented an effective information security program and practices since an overall maturity level of Level 4: Managed and Measurable was noted.

FY2022 Annual Cybersecurity Performance Summary

Office of Personnel Management

Framework	CIO Rating	IGRating
Identify	14.7	Defined
Protect	25.2	Consistently Implemented
Detect	5.8	Defined
Respond	15	Managed and Measurable
Recover	13.5	Defined
Overall	74%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	0	0	0
E-mail	0	1	0
External/Removable Media	0	0	0
Impersonation	0	0	0
Improper Usage	167	193	26
Loss or Theft of Equipment	9	0	1
Web	0	0	1
Other	32	67	30
Multiple Attack Vectors	0	0	0
Total	208	261	58

CIO Self-Assessment

Throughout the year, the OPM continued its effort to build a robust, adaptable, and cost-effective cybersecurity program. Notable efforts included a significant rewrite of the OPM’s cybersecurity policy to address the key elements of the Executive Order (EO) 14028, construction of an enterprise cybersecurity architecture aligning to zero-trust principles, strengthening the implementation of multifactor authentication services, implementing cyber threat intelligence and threat hunting capabilities, encryption of data in-transit, and continued adoption of cloud services.

Independent Assessment

The FY 2022 Core IG Metrics use a maturity model evaluation system derived from the NIST Cybersecurity Framework. The Cybersecurity Framework is comprised of five “function” areas that map to the nine “domains” under the function areas. These nine domains are broad cybersecurity control areas used to assess the effectiveness of the information security policies, procedures, and practices of the agency. In FY 2022, representatives from OMB, FCEB CISO teams, CIGIE, and IC Community selected 20 Core IG Metrics that should provide sufficient data to determine the effectiveness of an Agency’s information security program with a high level of confidence. These 20 Core IG Metrics were selected from each domain, which are the specific controls that we evaluated and tested when assessing the agency’s cybersecurity program. Each core metric receives a maturity level rating. Last year we requested OPM to conduct a self-assessment. This gave OPM the opportunity to document its current maturity level for each metric and the maturity level that it hopes to achieve by the end of FY 22. We validated OPM’s current maturity level throughout the fiscal year and reported on the results of our analysis. Risk Management - Maturity Level 3; SCRM - Maturity Level 1; Supply Chain Risk Management – Maturity Level 1; Configuration Management - Maturity Level 2; Identity, Credential, and Access Management - Maturity Level 2; Data Protection and Privacy - Maturity Level 3; Security Training - Maturity Level 3; Information Security Continuous Monitoring - Maturity Level 2; Incident Response - Maturity Level 4 and Contingency Planning - Maturity Level 2. In FY 2022, we assessed all metrics and OPM's overall maturity level as 3. Level 4, Managed and Measurable, is considered to be an effective level of security for the overall program level. Therefore, the information security program is deemed ineffective. Recommendations have been provided to assist in elevating the program's overall level.

FY2022 Annual Cybersecurity Performance Summary

Small Business Administration

Framework	CIO Rating	IGRating
Identify	13.1	Defined
Protect	33.5	Defined
Detect	9.4	Consistently Implemented
Respond	15	Managed and Measurable
Recover	15	Consistently Implemented
Overall	86%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	43	145	45
E-mail	1,694	772	1045
External/Removable Media	0	0	0
Impersonation	37	268	21
Improper Usage	494	245	157
Loss or Theft of Equipment	7	33	19
Web	415	612	665
Other	238	1,536	2331
Multiple Attack Vectors	1	9	0
Total	2,929	3,620	4283

CIO Self-Assessment

The SBA built, delivers, and continues to mature resilient and robust Enterprise Cybersecurity Service (ECS) capabilities that we can consistently implement, maintain, and leverage throughout the agency. These ECS capabilities align to cover areas such as cyber threat intelligence, network monitoring, penetration testing, risk management and assessment, vulnerability scanning and remediation, event log correlation, awareness training, and incident response.

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

Independent Assessment

We performed an independent evaluation on the effectiveness of the U.S. Small Business Administration (SBA) information security program and practices for FY 2022. Our scope included assessing the maturity levels for the OMB FY 2022 Core Inspector General Metrics Implementation Analysis and Guidelines at the entity level and for seven selected SBA information systems. Based on the work performed in FY 2022, we assessed the overall SBA information technology (IT) security program as not effective based on the definition in the FY 2022 Core IG Metrics. Specifically, we assessed the identify and Protect functions as Defined (level 2), the Detect, and Recover functions as Consistently Implemented (Level 3) and the Respond function as Managed and Measurable (Level 4).

We made recommendations in the Identify, Protect, Detect, and Recover Functions to improve the information security program. SBA should continue to design, implement, and monitor qualitative and quantitative key performance indicators to measure the effectiveness of its controls, processes, and activities. SBA should also develop and implement Plans of Action and Milestones (POA&Ms) to remediate the FY 2022 audit findings.

FY2022 Annual Cybersecurity Performance Summary

Social Security Administration

Framework	CIO Rating	IGRating
Identify	8.1	Defined
Protect	26.3	Consistently Implemented
Detect	5.2	Defined
Respond	15	Managed and Measurable
Recover	15	Consistently Implemented
Overall	70%	Not Effective

Incidents by Attack Vector	2020	2021	2022
Attrition	241	204	16
E-mail	42	31	18
External/Removable Media	3	1	1
Impersonation	43	2	0
Improper Usage	2,386	1,215	1116
Loss or Theft of Equipment	41	26	84
Web	1,800	1,859	944
Other	4,305	2,956	1252
Multiple Attack Vectors	17	16	0
Total	8,878	6,310	3431

CIO Self-Assessment

SSA's mission requires it to collect PII for over 325 million Americans. This information is vital to performing the agency's essential functions but makes its network, systems, and databases a rich target for adversaries. Protecting our networks and the information we use to administer our programs remains a critical priority. Many of our initiatives are in strong alignment with EO 14028, demonstrating that we are effectively prioritizing our IT resources to combat emerging cybersecurity threats. As evidenced via our improved FY 2022 scores, we continuously enhance our cybersecurity controls and elevate maturity levels. Specifically, in the IDENTIFY area of the NIST Framework, the Information System Security Officers enhanced security governance throughout the Agency by collaborating with regional system owners to define the critical security controls and developing system security plans for 23 regional systems that were successfully assessed. In the PROTECT area, SSA earned effective ratings in the Security Training and Data Protection and Privacy domains. We strengthened controls related to encryption of data at rest, data in transit, and media protections for internal systems in accordance with EO 14028. FISMA auditors acknowledged that SSA analyzes qualitative and quantitative measures on the performance of its data exfiltration and enhanced network defenses. In the DETECT area, we improved our mitigation of open network shared drives within our security incident response ticketing system which correlates open share findings with the agency's CMDB program. In the RESPOND area, we successfully demonstrated an effective and mature incident response program through our detection and handling of multiple cyber vulnerabilities. In the RECOVER area, we completed the biennial review and validation of the agency's Primary Mission Essential Function and submitted to the Federal Emergency Management Agency.

Independent Assessment

Although SSA established an Agency-wide information security program and practices, an independent auditor identified several deficiencies related to Risk Management; Supply Chain Risk Management; Configuration Management; Identity and Access Management; Information Security Continuous Monitoring; and Contingency Planning. The weaknesses identified may limit the Agency's ability to adequately protect the organization's information and information systems. In addition, the auditor assessed only two Federal Information Security Modernization Act of 2014 domain as Managed and Measurable (Level 4). The Fiscal Year 2022 Federal Information Security Modernization Act of 2014 Inspector General Reporting Metrics defines an effective information security program as Managed and Measurable (Level 4).