Office of Inspector General
Committee for Purchase from People Who Are Blind or Severely Disabled
(U.S. AbilityOne Commission OIG)

355 E Street SW (OIG Suite 335)
Washington, DC 20024-3243

December 6, 2022

MEMORANDUM

FOR: Jeffrey A. Koses
Chairperson
U.S. AbilityOne Commission

Kimberly M. Zeich
Executive Director
U.S. AbilityOne Commission

FROM: Stefania Pozzi Porter
Inspector General
U.S. AbilityOne Commission OIG

SUBJECT: Fiscal Year 2022 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act (FISMA)

I am pleased to provide the results of the annual independent evaluation of the Commission's Information Security Program and Practices for Fiscal Year (FY) 2022. The Office of Inspector General engaged the independent public accounting firm McConnell & Jones LLP (M&J) to conduct the annual evaluation and complete the FY 2022 IG FISMA Reporting Metrics.

The objective of the evaluation was to assess the compliance of the Commission's information security policies, procedures and standards and guidelines with the Federal Information Security Modernization Act (FISMA). The evaluators determined that although the Commission took positive steps to implement policies, procedures and strategies, there are existing improvement opportunities. Specifically, four recommendations from prior years remain open. Accordingly, the Commission needs to undertake corrective actions to remediate the open prior year recommendations. Furthermore, the overall assessment of the Commission's FY 2022 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. However, the evaluators identified four new findings with four corresponding recommendations. The four findings are as follows:

1. Supply chain policy was not in place for nine of ten months of this fiscal year's evaluation period.

2. There were a number of endpoints within the Commission that were not encrypted.
3. The Incident Report Plan has not been updated in more than three years.
4. A Business Impact Analysis (BIA) has not been completed.

We appreciate the Commission's assistance during the course of the engagement. If you have any questions, please contact Rosario A. Torres, CIA, CGAP, Assistant Inspector General for Auditing, at 703-772-9054 or at rtorres@oig.abilityone.gov.

cc: Amy Jensen
Deputy Executive Director (Acting)
U.S. AbilityOne Commission

Kelvin Wood
Chief of Staff
U.S. AbilityOne Commission

Edward Yang
Chief Information Officer
U.S. AbilityOne Commission

Office of the Inspector General

for

U.S. AbilityOne Commission

FY 2022 Evaluation of the U.S. AbilityOne Commission's Compliance with the Federal Information Security Modernization Act

October 24, 2022

McConnell Jones

Diverse Thinking | Unique Perspectives

McConnell Jones

October 24, 2022

Rosario Torres
Assistant Inspector General for Auditing
Office of Inspector General
U.S. AbilityOne Commission

We are pleased to provide our report on the information security at the U.S. AbilityOne Commission (Commission) for Fiscal Year 2022 (FY22). The objective of this independent evaluation was to assess the compliance of the Commission's information security policies, procedures and standards and guidelines with the Federal Information Security Modernization Act (FISMA). The scope of the evaluation focused on the Commission's General Support System (GSS) and related information security policies, procedures, standards and guidelines.

Under *FY22 Inspector General FISMA Reporting Metrics*, Inspectors General are required to assess the effectiveness of information security programs on a maturity model spectrum.

During FY22, there were four findings identified with four corresponding recommendations regarding the Commission's information security program which included:

1. Supply chain policy was not in place for nine of ten months of this fiscal year's evaluation period.
2. There were a number of endpoints within the Commission that were not encrypted.
3. The Incident Report Plan has not been updated in more than three years.
4. A Business Impact Analysis (BIA) has not been completed.

The guidance provides that in the context of the maturity model, a Level 4 – Managed and Measurable, is defined as an effective level for an information security program of an agency. The overall assessment of the Commission's FY 2021 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. At this level, the Commission took positive steps to implement policies, procedures and strategies; however, we are reporting that improvements are required. As of this report date, there are two open prior year recommendations each from FY20 and from FY21. We identified four new recommendations during the FY22 evaluation which are detailed within our report. The Commission's comments are included in **Attachment A**.

5101 Wisconsin Ave. NW
Suite 210
Washington, D.C. 20016
Phone: 202.207.3570
Fax: 202.846.6310

WWW.MCCONNELLJONES.COM

McConnell Jones

McConnell & Jones would like to thank the Office of the Inspector General (OIG) and the Commission's Information Technology (IT) office for their assistance in helping us meet the objective of our evaluation.

McConnell & Jones LLP

Table of Contents

Executive Summary

Pursuant to the Federal Information Modernization Act (FISMA), the U.S. AbilityOne Commission (Commission) Office of Inspector General (OIG) engaged McConnell & Jones to conduct the annual evaluation and complete the FY22 IG FISMA Reporting Metrics. The Commission OIG submitted the cyber metrics into CyberScope on July 27, 2022.

Under *FY 2022 Inspector General FISMA Reporting Metrics*, IGs are required to assess the effectiveness of information security programs on a maturity model spectrum. The guidance provides that in the context of the maturity model, a Level 4 - Managed and Measurable, is defined as effective level for information security program of an agency. As the Commission's programs are evaluated, the ratings at the function, domain and overall program levels drive the determination of effectiveness. The overall assessment of the Commission's FY22 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 table below summarizes the function and maturity level ratings for FY22 FISMA Metrics, as well as the overall rating from the CyberScope system.

FY22 FISMA Metrics from CyberScope		
Function	**Calculated Maturity Level**	**Assessed Maturity Level**
Function 1: Identify – Risk Management / Supply Chain Risk Management	4 - Managed and Measurable	1 - Ad Hoc
Function 2: Protect – Configuration Management / Identity & Access Management / Data Protection & Privacy / Security Training	4 - Managed and Measurable	4 - Managed and Measurable
Function 3: Detect – ISCM	4 - Managed and Measurable	4 - Managed and Measurable
Function 4: Respond – Incident Response	4 - Managed and Measurable	4 - Managed and Measurable
Function 5: Recover – Contingency Planning	3 - Consistently Implemented	3 - Consistently Implemented
Overall	Effective	Effective

Our findings and recommendations will improve the Commission's IT security and privacy operations and its compliance with FISMA functional areas. The table below summarizes our FY22 findings by control, condition and the number of recommendations.

FY22 FISMA Findings		
Control #	**Condition**	**Recommendations**
SR-3	The supply chain policy was not in place for nine of ten months of this fiscal year's evaluation period.	1
SC-28	There were a number of endpoints within the Commission that were not encrypted.	1
IR-8	The Incident Response Plan has not been updated in three years.	1
CP-2	A Business Impact Analysis (BIA) has not been completed.	1

The Commission's management and IT organization remain responsible for following-up on all recommendations and implementation of corrective actions.

Background

McConnell & Jones, on behalf of the OIG, conducted an independent evaluation of the Commission's information security program and the information security program's compliance with applicable federal computer security laws and regulations. This report was prepared by McConnell & Jones and derived from the *FY 2022 Inspector General FISMA Reporting Metrics*, and the evaluation guide that provides test objectives and procedures.

On December 17, 2002, the E-Government Act of 2002 (Public Law 107-347) was enacted. This Act was subsequently amended by the Federal Information Security Modernization Act of 2014 (Public Law 113-283), commonly referred as FISMA. FISMA requires federal agencies to develop, document and implement an agency-wide information security program that provides security for information and information systems that support the operations and assets of the Commission. This program includes providing security for information systems provided or managed by another agency, contractor or other source. FISMA is supported by security policy promulgated through OMB, and risk-based standards and guidelines published in the National Institute of Standards and Technology (NIST), Special Publication (SP) series.

Implementing adequate information security controls is essential to ensuring an organization can effectively meet its mission. Under FISMA, agency heads are responsible for providing information security protections commensurate with the risk and magnitude of harm resulting from the unauthorized access, use, disclosure, disruption, modification or destruction of information and information systems. FISMA requires agencies to have an annual independent evaluation of their information security programs and practices and to report the evaluation results to OMB. FISMA requires that the independent evaluation be performed by the Commission IG, or an independent external auditor as determined by the IG.

Scope and Methodology

The scope of our testing focused on the Commission's General Support System (GSS) and related information security policies, procedures, standards and guidelines. We conducted testing through inquiry of Commission IT personnel, observation of activities, inspection of relevant documentation, and the performance of technical security testing. Our testing covered a sample of controls as listed in NIST SP 800-53, Rev. 5, *Security and Privacy Controls for Information Systems and Organizations*, and prior year implemented recommendations. Testing covered system security plans, access controls, risk assessments, personnel security, contingency planning, identification, authentication and auditing. Our testing covered the period October 1, 2021 through July 31, 2022 (FY22).

For purposes of the FY22 FISMA evaluation, we reviewed 17 control families and 57 associated controls. The scope of our testing included the following new controls, along with testing of the controls from the prior year:

FY22 Controls to be Evaluated	
Control Number	**Control Name**
Access Control	
AC-1	Policies and Procedures
AC-2	Account Management
AC-5	Separation of Duties
AC-6	Least Privilege
AC-17	Remote Access
Awareness and Training	
AT-2	Literacy Training and Awareness
AT-3	Role-Based Training
Audit and Accountability	
AU-2	Event Logging
AU-3	Content of Audit Records
AU-6	Audit Record Review, Analysis, and Reporting
Certification, Accreditation, and Security Assessments	
CA-2	Control Assessments
CA-3	Information Change
CA-5	Plan of Action and Milestones
CA-6	Authorization
CA-7	Continuous Monitoring
Configuration Management	
CM-3	Configuration Change Control
CM-6	Configuration Settings
CM-7	Least Functionality
CM-8	System Component Inventory
CM-10	Software Usage Restrictions
CM-11	User-Installed Software
Contingency Planning	
CP-2	Contingency Plan
CP-3	Contingency Training
CP-4	Contingency Plan Testing
Identification and Authentication	
IA-2	Identification and Authentication
IA-4	Identifier Management
IA-5	Authenticator Management
IA-8	Identification and Authentication (Non-Organizational Users)

FY22 Controls to be Evaluated	
Control Number	**Control Name**
Incident Response	
IR-4	Incident Handling
IR-5	Incident Monitoring
IR-6	Incident Reporting
Media Protection	
MP-3	Media Marking
MP-6	Media Sanitization
Physical and Environmental Protection	
PE-3	Physical Access Control
Planning	
PL-2	System Security and Privacy Plans
Program Management	
PM-5	System Inventory
PM-6	Measures of Performance
PM-9	Risk Management Strategy
PM-10	Authorization Process
PM-13	Security and Privacy Workforce
PM-14	Testing, Training, and Monitoring
PM-31	Continuous Monitoring Strategy
Risk Assessment	
RA-3	Risk Assessment
RA-5	Vulnerability Monitoring and Scanning
RA-9	Criticality Analysis
System and Services Acquisition	
SA-4	Acquisition Process
Systems and Communications Protection	
SC-7	Boundary Protection
SC-8	Transmission Confidentiality and Integrity
SC-18	Mobile Code
SC-28	Protection of Information at Rest

FY22 Controls to be Evaluated	
Control Number	**Control Name**
System and Information Integrity	
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	System Monitoring
SI-7	Software, Firmware, and Information Integrity
Supply Chain Risk Management	
SR-3	Supply Chain Controls and Processes
SR-5	Acquisition Strategies, Tools, and Methods
SR-6	Supplier Assessments and Reviews

Current Year Findings

The results of our FY22 FISMA evaluation identified four findings related to the FISMA controls evaluated, and we provide four associated recommendations as noted below.

1. Supply Chain Deficiency

Condition:

The supply chain policy was not in place for nine months of the ten-month evaluation period.

Due to the new reporting deadline of July 31, 2022, the FY22 evaluation period covered the 10 months from October 1, 2021 through July 31, 2022. The Commission deployed a supply chain policy on July 1, 2022.

Criteria:

NIST 800-53 Rev. 5, SR-3 Supply Chain Controls and Processes

Control:

a. Establish a process or processes to identify and address weaknesses or deficiencies in the supply chain elements and processes of [Assignment: organization-defined system or system component] in coordination with [Assignment: organization-defined supply chain personnel];

b. Employ the following controls to protect against supply chain risks to the system, system component, or system service and to limit the harm or consequences from supply chain related events: [Assignment: organization-defined supply chain controls]; and

c. Document the selected and implemented supply chain processes and controls in [Selection: security and privacy plans; supply chain risk management plan; [Assignment: organization defined document]].

Cause:

This is a new control and the Commission needed time to develop the policy, as well as deploy the relevant stipulations within the policy.

Risk:

Without an appropriate supply chain Policy in place, there is the risk that the Commission will be unprepared for and unable to respond expeditiously in the event that supply chain issues affect the Commission.

Recommendation:

We recommend that the Commission IT staff evaluate the Supply Chain policy against the requirements of NIST 800-53 Rev. 5 to ensure compliance for each of the individual controls.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's completed actions which were accomplished by July 1, 2022.

Auditor's Response to Management's Comments

Finding 01, Recommendation 1

The Commission is responsible to implement a supply chain policy, and we verified that the policy was prepared and put in place as noted. The OIG and Auditors will review and evaluate the implementation and sustainment of the policy in future evaluations.

2. Device Encryption Deficiency

Condition:

As of July 31, the Commission had endpoint devices that were not encrypted.

The Commission IT staff provided a stale inventory listing of encrypted devices (dated July 5, 2022), which included inactive devices that were no longer within the Commission's device inventory at that time. The Commission IT staff subsequently provided an updated listing which reflected these inactive devices were removed. This inventory listing was dated August 15, 2022, which is after the conclusion of the FISMA evaluation period (July 31, 2022).

Thus, for purposes of the evaluation period-end, this condition existed, but it was immediately resolved shortly thereafter.

Criteria:

NIST 800-53, Revision 5, Protection of Information at Rest (SC-28) states:

Control: Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Cause:

The IT Department did not configure the endpoints for all devices pursuant to the NIST criteria cited above.

Risk:

By having some endpoints without encryption, the Commission runs the risk of having sensitive data presented in clear text as some of the endpoints are not encrypted. This ultimately could result in data loss exposure to the Commission.

Recommendation(s):

This finding is closed as the Commission IT staff encrypted all devices and resolved this finding as of August 15, 2022. However, we recommend that the Commission IT staff regularly review the inventory of encrypted devices to ensure that it reflects the current inventory status. Additionally, we recommend that a copy of the inventory listing be compiled and maintained as of July 31st of each year.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's completed actions which were accomplished by August 15, 2022.

Auditor's Response to Management's Comments

Finding 02, Recommendation 1

The Commission is responsible to maintain the device inventory and to ensure that these devices are and remain encrypt. The OIG and Auditors will review and evaluate the inventory and sustainment of their encryption in future evaluations.

3. Incident Response Plan Deficiency

Condition:

The Incident Response Plan has not been updated in more than three years.

Criteria:

NIST 800-53, Revision 5, Incident Response Plan (IR-8) states:

c. Update the incident response plan to address system and organizational changes or problems encountered during plan implementation, execution, or testing

Cause:

The Commission IT staff did not update the Incident Response Plan according to the guidance set forth in the NIST criteria cited above.

Risk:

By not having an up-to-date Incident Response Plan, the Plan may not reflect the latest operating environment or most efficient response procedures, thereby increasing the risk of prolonging an incident.

Recommendation(s):

Review and update the Incident Response Plan annually.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's plan to review and updated the Incident Response Plan by December 30, 2022.

Auditor's Response to Management's Comments

Finding 03, Recommendation 1

The Commission is responsible for preparing and implementing an Incident Response Plan. The OIG and Auditors will review and evaluate the Incident Response Plan, it's implementation, sustainment and the monitoring and updating of it in future evaluations.

4. Business Impact Analysis Deficiency

Condition:

A Business Impact Analysis (BIA) has not been completed for the GSS.

Criteria:

NIST 800-53, Revision 5, Contingency Plan (CP-2) states:

8) Identify critical system assets supporting [Selection: all; essential] mission and business functions.

Cause:

The Commission IT staff did not complete the BIA according to the guidance set forth in the NIST criteria cited above.

Risk:

By not preparing a BIA, there is the increased risk that the Commission has not determined and evaluated the potential effects of an interruption to critical business operations as a result of a disaster, accident or emergency.

Recommendation(s):

Ensure that a BIA is prepared, completed and approved. After the initial BIA is put in place, it should be updated whenever significant updates to the GSS are implemented.

Management Response:

The Commission concurred with the finding and recommendations. Management's comments are included in **Attachment A**, which details the Commission's response on that the BIA was put in place in 2016.

Auditor's Response to Management's Comments

Finding 03, Recommendation 1

The Commission is responsible for preparing, implementing and periodically updating the BIA. Although management states the BIA was in place, the auditors found that the BIA was not in place during the performance of our audit. If there is a BIA from 2016, the OIG and Auditors recommend that it be updated due to it being over six years old. Given that management believes it was implemented, the OIG and Auditors will review and evaluate the subject BIA in future evaluations.

Prior Year Findings

During the FY22 engagement, we reviewed the corrective action status of the findings and recommendations from the FY20 and FY21 evaluations. The results of our evaluation revealed that these recommendations remain unresolved as of the July 31, 2022, which is the end of the FY22 FISMA evaluation period.

At the conclusion of the FY21 FISMA evaluation, there were two open recommendations which carried forward from the FY20 FISMA evaluation. These recommendations remain open as of July 31, 2022. Additionally, the FY21 FISMA evaluation had two recommendations as well, and these recommendations also remain open as of July 31, 2022.

The Commission IT staff needs to undertake corrective actions to implement these recommendations from the prior years' evaluations.

For recommendations 2020-1, 2020-2 and 2021-1, each of the related controls were within the scope of the FY22 evaluation. The audit evidence provided by the Commission IT staff was assessed for each of these controls within the scope of our FY22 testing. We attempted to determine whether these had been remediated. Based upon our examination of these controls and the associated audit evidence, we noted that these findings (or conditions) were not remediated and remained open as of July 31, 2022.

For recommendation 2021-2, the related control was not within the scope of our FY22 evaluation. Thus, we requested audit documentation to allow us to assess the remediation status of this prior year finding. We evaluated the documentation provided by the Commission IT staff, and we noted that the finding (or condition) was not remediated and remained open as of July 31, 2022.

The table below details the status of the prior years' open recommendations:

STATUS OF PRIOR YEARS FISMA RECOMMENDATIONS

Status of Recommendations	Year / Rec. #	Status
Risk Assessment		
The Commission should follow their vulnerability remediation policies.	2020-1	Open
Scanning should be run on a monthly basis, however, if there are medium and/or high vulnerabilities, then they should be remediated, and the scan should be repeated and run again.	2020-2	Open
Security Assessment and Authorization		
Vulnerabilities not being remediated in a timely manner.	2021-1	Open
Configuration settings are not in compliance with Commission policies.	2021-2	Open

Attachment A – Commission's Comments

Please refer to the Commission's comments below, which detail management's concurrence, planned actions and estimated completion dates to address the open findings and recommendations.

U.S. ABILITYONE COMMISSION

October 21, 2022

PHONE: 703-603-7740

Patriots Plaza III
355 E Street, SW - Suite 325
Washington, DC 20024

Ms. Stefania Porter
Inspector General
AbilityOne Office of Inspector General (OIG)
Committee for Purchase from People
Who Are Blind or Severely Disabled

Dear Ms. Porter:

The Commission has reviewed the results of the FY 22 OIG assessment of its Information Systems and its compliance with the Federal Information Security Modernization Act of 2014 (FISMA). The Commission concurs with the OIG findings. Below are the Commission's proposed actions and estimated timelines for completion.

(1) Recommendation #1: Supply Chain Deficiency

The supply chain policy was not in place for nine months of the ten-month evaluation period.

Response: AbilityOne Supply Chain policy has been reviewed and signed in accordance with the requirements of NIST 800-53 Rev. 5; copy provided by separate action.

(2) Recommendation #2: Device Encryption Deficiency

As of July 31, the Commission had endpoint devices that were not encrypted.

Response: This finding is closed as the Commission IT staff encrypted all devices and resolved.

(3) Recommendation #3: Incident Response Plan Deficiency

The Incident Response Plan has not been updated in more than three years.

Response: The IR will be reviewed and updated as needed within 60 days.

(4) Recommendation #4: Business Impact Analysis Deficiency

A Business Impact Analysis (BIA) has not been completed for the GSS.

Response: The Commission's BIA for the General Support System (GSS) was completed September 1, 2016, and rated as "Moderate Level"; copy provided by separate action.

COMMITTEE FOR PURCHASE FROM PEOPLE WHO ARE BLIND OR SEVERELY DISABLED
An Independent Federal Agency

Type text here

The Agency appreciates the support and recommendations provided by the OIG throughout this engagement to enhance our Cybersecurity posture. We will continue to invest in increased IT and Cybersecurity protection controls to increase our NIST Cybersecurity maturity rating.

Sincerely,

Kelvin R. Wood
Chief of Staff
Authorizing Official

cc: System Owner
Chief Information Officer
Chief Information Security Officer